User Manual
v.1.1

Webee™

Wireless N Router

with 3G Modem Support

CONTENTS

1. INTRODUCTION

The Webee Wireless N Router offers you a high-speed WiFi network and internet access via a fixed or 3G broadband modem.

You can connect the router to an xDSL Modem (usually ADSL or VDSL), Cable Modem or 3G USB Modem.

You can also connect a USB memory stick or external hard disk drive to the router and share files among the users in a local network.

The router is ready for use without changing the factory default settings. However, for wireless data security we recommend the following settings: changing of the network name (SSID), setting the encryption mode for the wireless network traffic and setting a user name and password in the router.

In the installation form you can collect the installation information for further use.

This document describes the steps required for the initial IP address assign and other Webee Wireless N Router configuration.

2. PRODUCT INFORMATION

2.1. PACKAGE CONTENTS

- Wireless Access Point / Router
- DC Power Adapter
- RJ-45 Cable Line (Cat5)
- Documentation CD

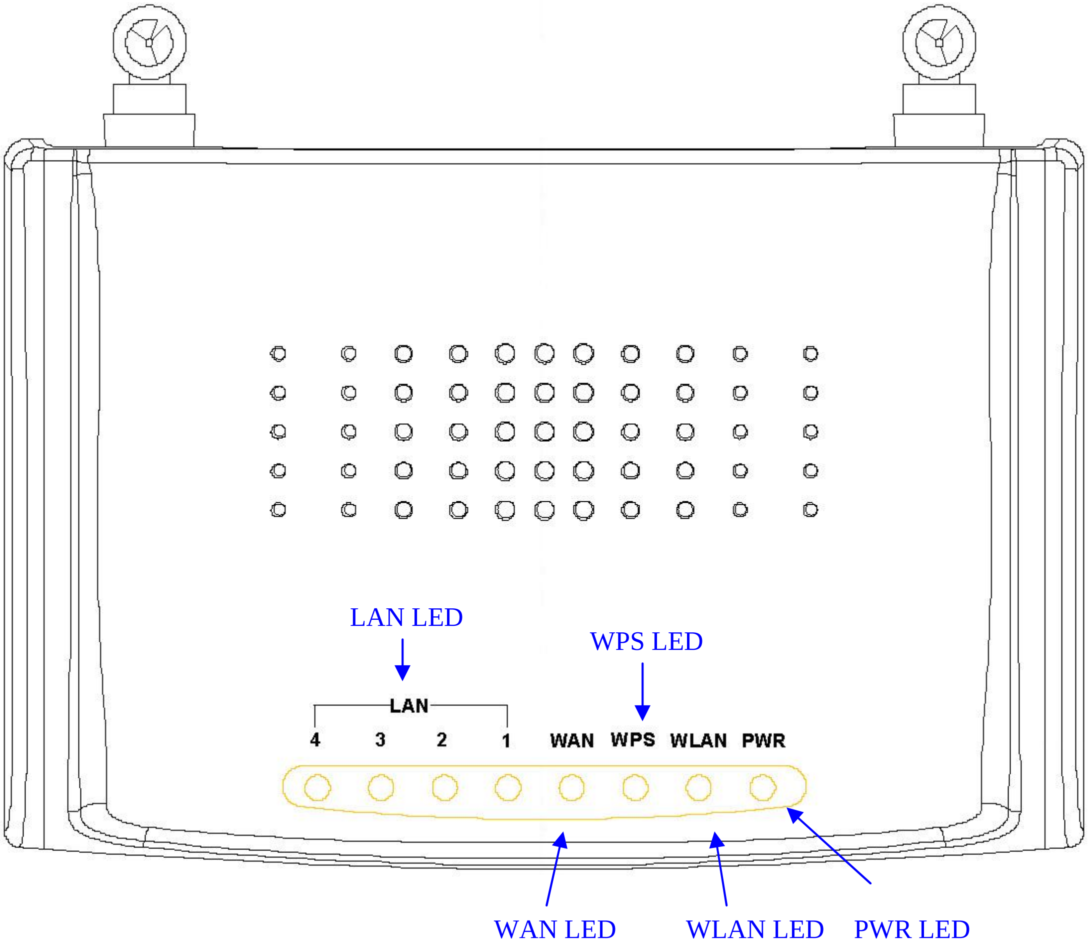
2.2. TECHNICAL SPECIFICATIONS

Product Name	Webee Wireless N Router Type 2
Standard	802.11b/g/n(Wireless), 802.3(10BaseT), 802.3u(100BaseT)
Data Transfer Rate	1,2,5.5,6,9,11,12,18,24,36,48,54, and maximum of 300Mbps
Modulation Method	BPSK/QPSK/16-QAM/64-QAM
Frequency Band	2.4GHz – 2.497GJz ISM Band, DSSS
RF Output Power	< 14dBm(802.11n),< 17dBm(802.11b),< 14dBm(802.11g)
Receiver Sensitivity	802.11b: -80dBm@8%, 802.11g: -70dBm@10%, 802.11n: -64dBm@10%
Operation Range	Indoor@Up to 100 meters,Outdoor@Up to 280 meters
Antenna	External Antenna(2Tx2R)
LED	Power, Active (WLAN), (Ethernet)
Security	64 bit/128 bit WEP, TKIP, AES
WAN Interface	One 10/100BaseT with RJ45 port
LAN Interface	Four 10/100BaseT with RJ45 port
USB Interface	One USB 2.0 Port
Power Consumption	DC Power Adapter
Operating Temperature	0 ~ 50^{o}C ambient temperature
Storage Temperature	-10 ~ 70°C ambient temperature
Humidity	5 to 90 % maximum (non-condensing)
Dimension	138x92x33mm

2.3. PRODUCT FEATURES

- Compatible with IEEE 802.11n specifications provides wireless speed up to 300Mbps data rate.
- Compatible with IEEE 802.11g high rate standard to provide wireless Ethernet speeds of 54Mbps data rate.
- Maximizes the performance and ideal for media-centric applications like streaming video, gaming and Voice over IP technology.
- Supports multi-operation (bridge/gateway/WISP) modes between wireless and wired Ethernet interfaces.
- Supports WPS, 64-bit and 128-bit WEP, WPA, WPA2 encryption/decryption and WPA with Radius function to protect the wireless data transmission.
- Supports IEEE 802.1x Authentication.
- Supports IEEE 802.3x full duplex flow control on 10/100M Ethernet interface.
- Supports DHCP server to provide clients auto IP addresses assignment.
- Supports DHCP client, static IP, PPPoE, PPTP L2TP, GSM 3.5G of WAN Interface.
- Supports firewall security with Port filtering, IP filtering, MAC filtering, Port forwarding, DMZ hosting, URL filtering and Virtual Server functions.
- Supports WEB based management and configuration.
- Supports UPnP for automatic Internet access.
- Supports Dynamic DNS service.
- Supports NTP client service.
- Supports Log table and remote Log service.
- Support Setup Wizard mode.
- Supports Network File sharing function.
- Supports FTP Server function.
- Supports USB storage format tool.

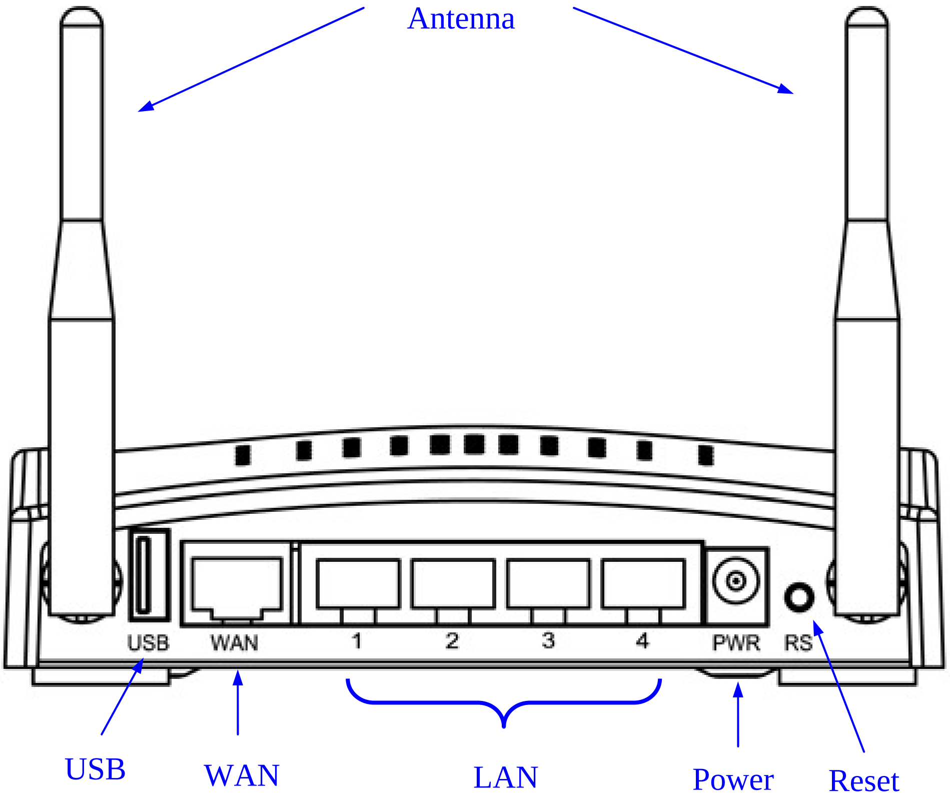
2.4. THE FRONT PANEL



LED Indicator	Status	Description
1. PWR LED	On	The Router is powered on.
	Off	The Router is powered off.
2. WLAN LED	Flashing	Data is transmitting or receiving on the antenna.
	Off	No data is transmitting or receiving on the antenna.
3. WPS LED	On	The WPS feature is Enabled.
	Off	The WPS feature is Disabled.
4. WAN LED	Flashing	Data is transmitting or receiving on the WAN interface.
	On	Port linked.
	Off	No link.
5. LAN LED	Flashing	Data is transmitting or receiving on the LAN interface.

	On	Port linked.
	Off	No link.

2.5. THE BACK PANEL



Interface	Description
Antenna (Fixed / SMA)	The Wireless LAN Antenna
PWR (Power)	The power jack allows an external DC power supply connection. The external DC adaptor provide adaptive power requirement to the Webee Router.
LAN	The RJ-45 sockets allow LAN connection through Category 5 cables. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
WAN	The RJ-45 socket allows WAN connection through a Category 5 cable. Support auto-sensing on 10/100M speed and half/ full duplex; comply with IEEE 802.3/ 802.3u respectively.
USB	The USB port allows USB Storage connection to support FTP server、File server.

RS (Reset)	Push continually the reset button 5 ~ 10 seconds to reset the configuration parameters to factory defaults.

2.6. HARDWARE REQUIREMENTS FOR WI-FI CONNECTIVITY

To use the Webee Router in a wireless local area network you will need:

1) Computer with an Ethernet interface
2) Ethernet Network Cable (RJ-45) (included in the package) to connect the router to a WAN interface. You may also use the network cable to connect the router to your computer during the installation.
3) Wireless Network Adapter if you wish to wirelessly connect your computer to the router

2.7. INSTALLATION FORM

Collect Installation Information:

WAN configuration (Contact your ISP or network administrator for this information)

○ ***DHCP Client***

○ ***Static IP***

IP Address	□□□ . □□□ . □□□ . □□□
Subnet Mask	□□□ . □□□ . □□□ . □□□
Default Gateway	□□□ . □□□ . □□□ . □□□
DNS Address	□□□ . □□□ . □□□ . □□□

LAN configuration

IP Address	**192. 168. 1. 254**
Subnet Mask	**255. 255 .255. 0**

IP Address	□□□ . □□□ . □□□ . □□□
Subnet Mask	□□□ . □□□ . □□□ . □□□

WLAN configuration

SSID	
Mode	
Channel Number	
Encryption	
Pass phrase	

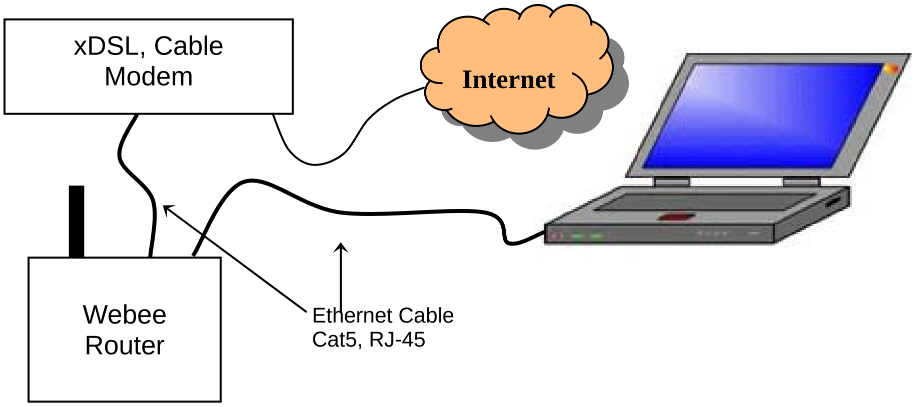
User name and password

Name	
Password	

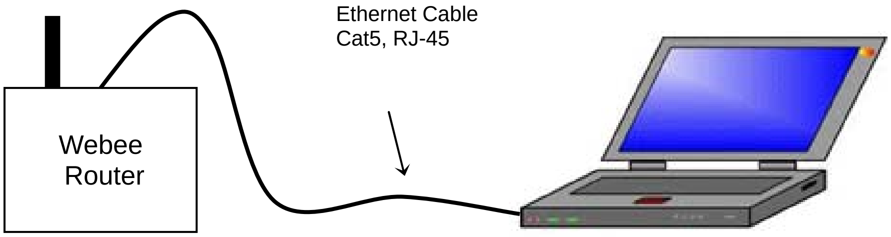
2.8. CONNECTION EXAMPLES

You can connect the router during the installation as show the following examples.

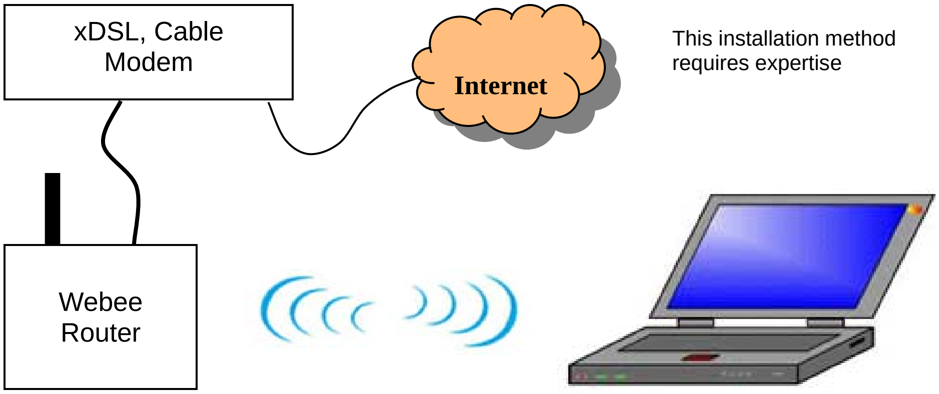
1. Connecting the Router to a computer in a local area network



2. Connecting the Router to a computer using a network cable



3. Wirelessly connecting the Router



This installation method requires expertise

3. INSTALLATION

3.1. HARDWARE INSTALLATION

Step 1: Place the Webee Router to the optimum transmission location. The best transmission location for your wireless router is usually at the geographic center of your wireless network, with the line of sight to all of your mobile stations.

Step 2: Connect the Webee Router to your wired network. Connect the Ethernet WAN interface of the router by category 5 Ethernet cable to your switch/ hub/ xDSL modem/ Cable modem. A straight-through Ethernet cable with appropriate cable length is needed.

Step 3: Supply DC power to the Webee Router. Use only the AC/DC power adapter supplied with the router; damage may occur if using a different type of power adapter.

The hardware installation is finished.

3.2. SOFTWARE INSTALLATION

There is no software drivers, patches or utilities installation needed, but only the configuration setting. Please refer to chapter 4 for software configuration.

Notice: It will take about 50 seconds to complete the boot up sequence after powered on the Router; Power LED will be active, and after that the WLAN LED will be flashing to show the WLAN interface is enabled and working now.

4. SOFTWARE CONFIGURATION

There are web based management and configuration functions allowing you to have the job done easily.

The Webee Router is delivered with the following factory default parameters on the Ethernet LAN interfaces.

Default IP Address**: *192.168.1.254***
Default IP subnet mask**: *255.255.255.0***
WEB login User Name**: *<blank>***
WEB login Password**: *<blank>***

4.1. PREPARE YOUR PC TO CONFIGURE THE ROUTER

For OS of Microsoft Windows XP:

1. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
2. Move mouse and double-click the right button on ***Network and Dial-up Connections*** icon. Move mouse and double-click the ***Local Area Connection*** icon. The ***Local Area Connection*** window will appear. Click ***Properties*** button in the ***Local Area Connection*** window.
3. Check the installed list of ***Network Components***. If TCP/IP is not installed, click the ***Add*** button to install it; otherwise go to step 6.
4. Select ***Protocol*** in the ***Network Component Type*** dialog box and click ***Add*** button.
5. Select ***TCP/IP*** in ***Microsoft*** of ***Select Network Protocol*** dialog box then click OK button to install the TCP/IP protocol, it may need the Microsoft Windows CD to complete the installation. Close and go back to ***Network*** dialog box after the TCP/IP installation.
6. Select ***TCP/IP*** and click the ***properties*** button on the ***Network*** dialog box.
7. Select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**
8. Click OK to complete the IP parameters setting.

For OS of Microsoft Windows Vista:

1 Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The Control ***Panel*** window will appear.

2 Move mouse and double-click the right button on ***Network Connections*** item. The ***Network Connections*** window will appear. Double click ***Local Area Connection*** icon, then ***User Account Control*** window will appear. Right click the ***Continue*** button to set properties.

3 In the ***Local Area Connection Properties*** window, select ***Networking*** tab, move mouse and click ***Internet Protocol Version 4 (TCP/IPv4)***, then click

Properties button.

4 Move mouse and click ***General*** tab, select ***Specify an IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ IP Subnet Mask: **255.255.255.0**

5. Click OK to complete the IP parameters setting.

For OS of Microsoft Windows 7:

1 Click the ***Start*** button and select ***Control Panel***. The ***Control Panel*** window will appear.

2 Move mouse and click the ***Network and Sharing Center*** item. Click **Change adapter settings**. The ***Local Area Connections*** icon will appear. Double click the ***Local Area Connection*** icon, then ***Local Area Connection Status*** window will appear. Click ***Properties*** button to set properties.

3 In the ***Local Area Connection Properties*** window, select ***Networking*** tab, move mouse and click ***Internet Protocol Version 4 (TCP/IPv4)***, then click ***Properties*** button.

4 Move mouse and click ***General*** tab, select ***Use the following IP address*** and type in values as following example.
   - ✓ IP Address: **192.168.1.1**, any IP address within 192.168.1.1 to 192.168.1.253 is good to connect the Wireless LAN Access Point.
   - ✓ Subnet Mask: **255.255.255.0**

5. Click OK to complete the IP parameters setting.

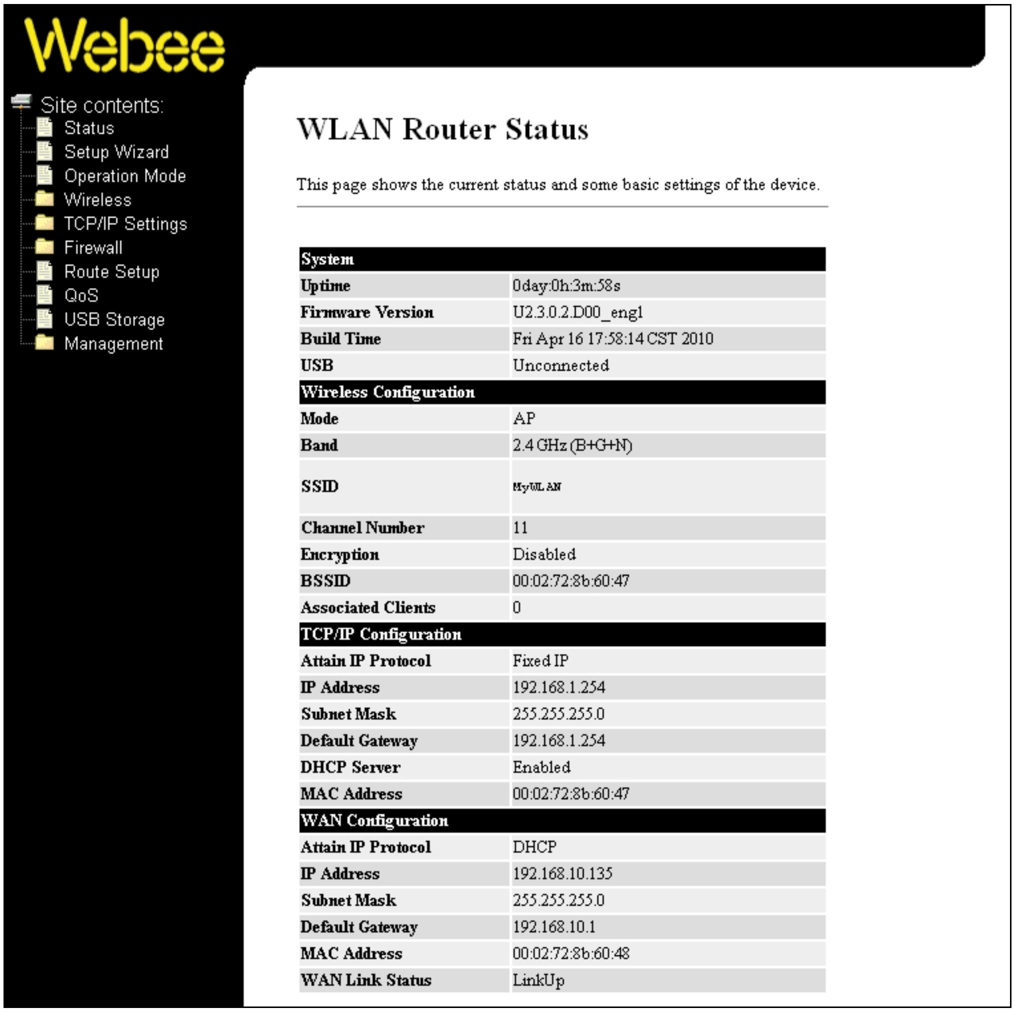
4.2. CONNECT TO THE ROUTER

Open your WEB browser and then enter **192.168.1.254** on the URL to connect the Router.

4.3. MANAGEMENT AND CONFIGURATION ON THE ROUTER

4.3.1 Status

This page shows the current status and some basic settings of the device, including system, wireless, Ethernet LAN and WAN configuration information.



WLAN Router Status

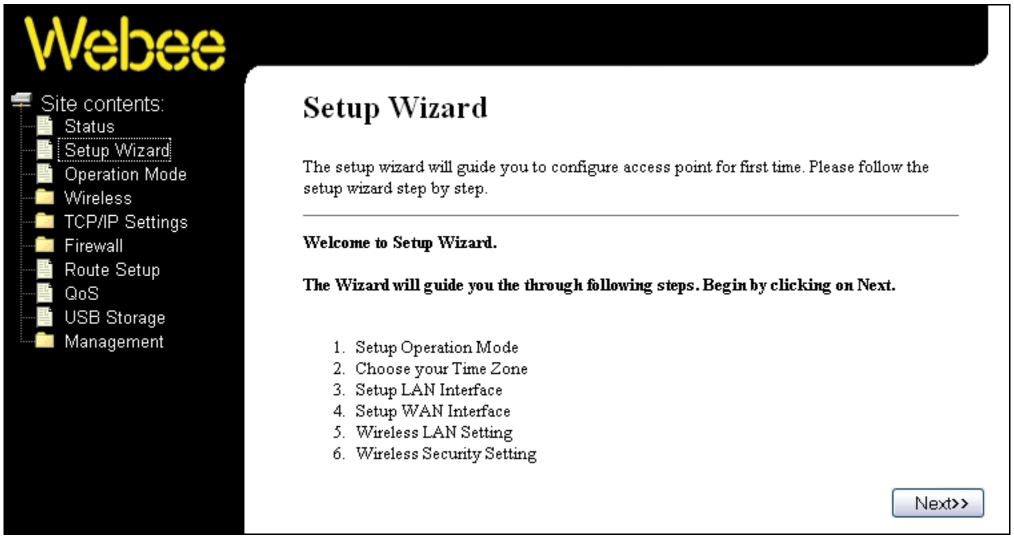
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:3m:58s
Firmware Version	U2.3.0.2.D00_eng1
Build Time	Fri Apr 16 17:58:14 CST 2010
USB	Unconnected
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	MyWLAN
Channel Number	11
Encryption	Disabled
BSSID	00:02:72:8b:60:47
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	Enabled
MAC Address	00:02:72:8b:60:47
WAN Configuration	
Attain IP Protocol	DHCP
IP Address	192.168.10.135
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
MAC Address	00:02:72:8b:60:48
WAN Link Status	LinkUp

Item	Description
System	
Uptime	It shows the duration since the Router is powered on.
Firmware version	It shows the firmware version of the Router.
Build time	It shows the Build-up time of firmware
USB	It shows USB connection status.
Wireless configuration	
Mode	It shows wireless operation mode
Band	It shows the current wireless operating frequency.
SSID	It shows the SSID of the Router. The SSID is the unique name of the Router and shared among its service area, so all devices attempts to join the same wireless network can identify it.
Channel Number	It shows the wireless channel connected currently.
Encryption	It shows the status of encryption function.
BSSID	It shows the BSSID address of the Router. BSSID is a six-byte address.
Associated Clients	It shows the number of connected clients (or stations, PCs).
TCP/IP configuration	
Attain IP Protocol	It shows type of connection.
IP Address	It shows the IP address of LAN interfaces of the Router.
Subnet Mask	It shows the IP subnet mask of LAN interfaces of the Router.
Default Gateway	It shows the default gateway setting for LAN interfaces outgoing data packets.
DHCP Server	It shows the DHCP server is enabled or not.
MAC Address	It shows the MAC address of LAN interfaces of the Router.
WAN configuration	
Attain IP Protocol	It shows how the Router gets the IP address. The IP address can be set manually to a fixed one or set dynamically by DHCP server or attain IP by PPPoE / PPTP /GSM 3.5G connection.
IP Address	It shows the IP address of WAN interface of the Router.
Subnet Mask	It shows the IP subnet mask of WAN interface of the Router.
Default Gateway	It shows the default gateway setting for WAN interface outgoing data packets.
MAC Address	It shows the MAC address of WAN interface of the Router.
WAN Link Status	It shows WAN connection status.

4.3.2 Setup Wizard

This page guides you to configure the wireless broadband router for the first time



Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

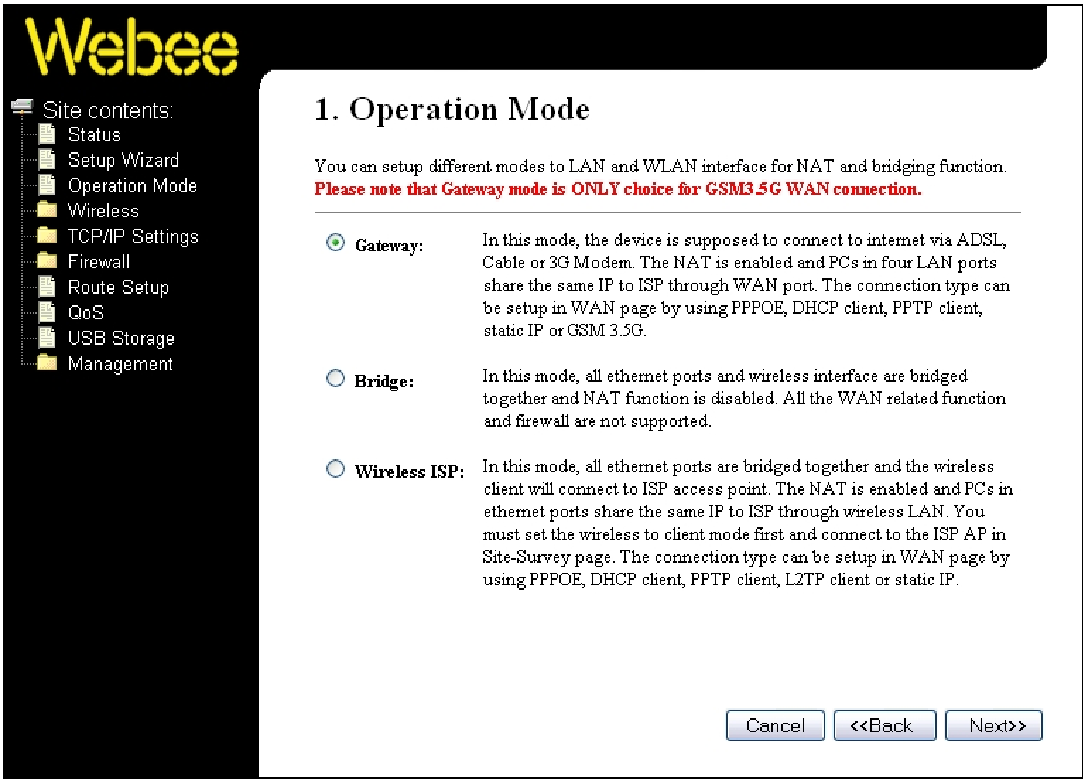
Welcome to Setup Wizard.

The Wizard will guide you the through following steps. Begin by clicking on Next.

1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Interface
5. Wireless LAN Setting
6. Wireless Security Setting

Operation Mode

This page followed by Setup Wizard page to define the operation mode.



1. Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Please note that Gateway mode is ONLY choice for GSM3.5G WAN connection.

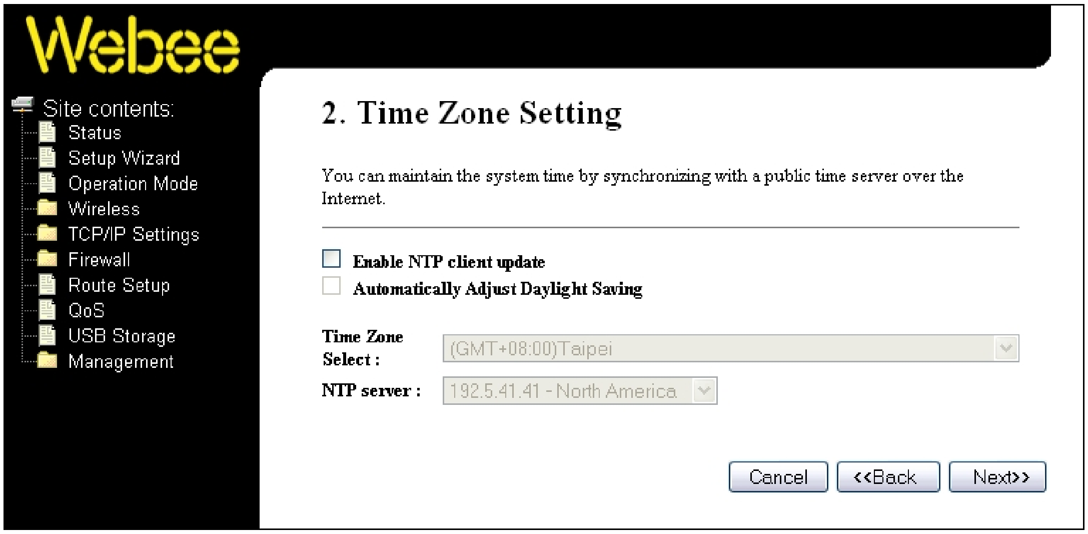
● **Gateway:** In this mode, the device is supposed to connect to internet via ADSL, Cable or 3G Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, static IP or GSM 3.5G.

○ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Time Zone Setting

This page is used to enable and configure NTP client



2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

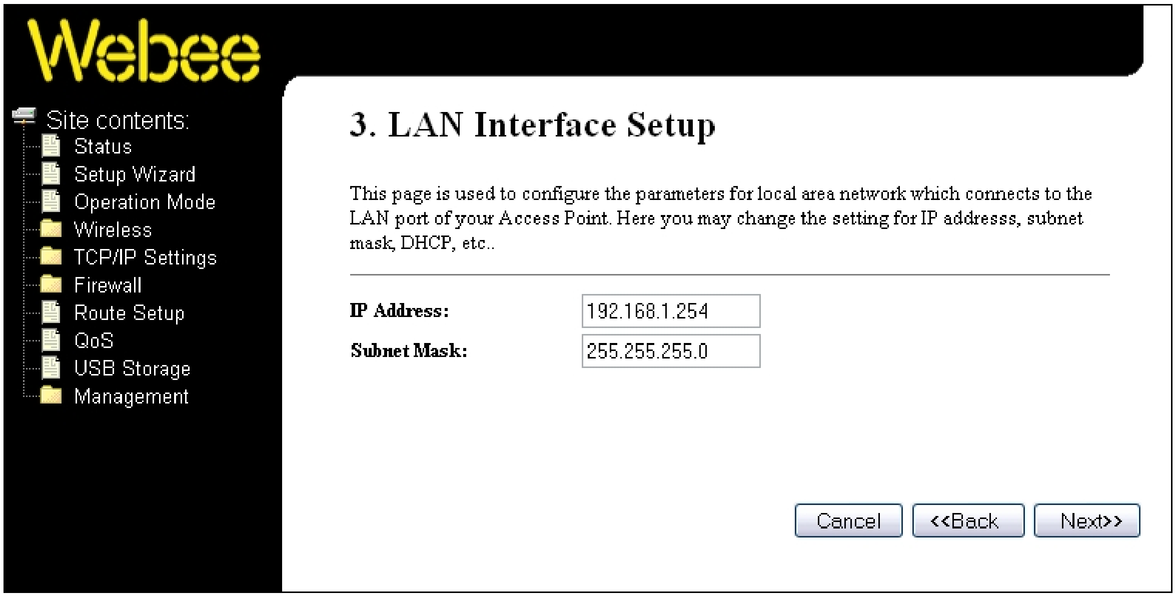
□ Enable NTP client update
□ Automatically Adjust Daylight Saving

Time Zone Select : (GMT+08:00)Taipei

NTP server : 192.5.41.41 - North America

LAN Interface Setup

This page is used to configure local area network IP address and subnet mask



3. LAN Interface Setup

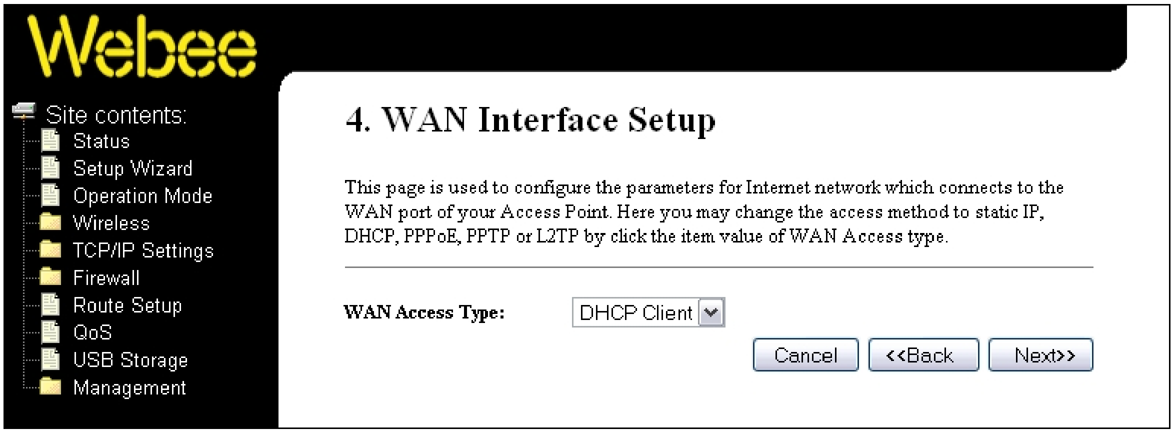
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

WAN Interface Setup

This page is used to configure WAN access type



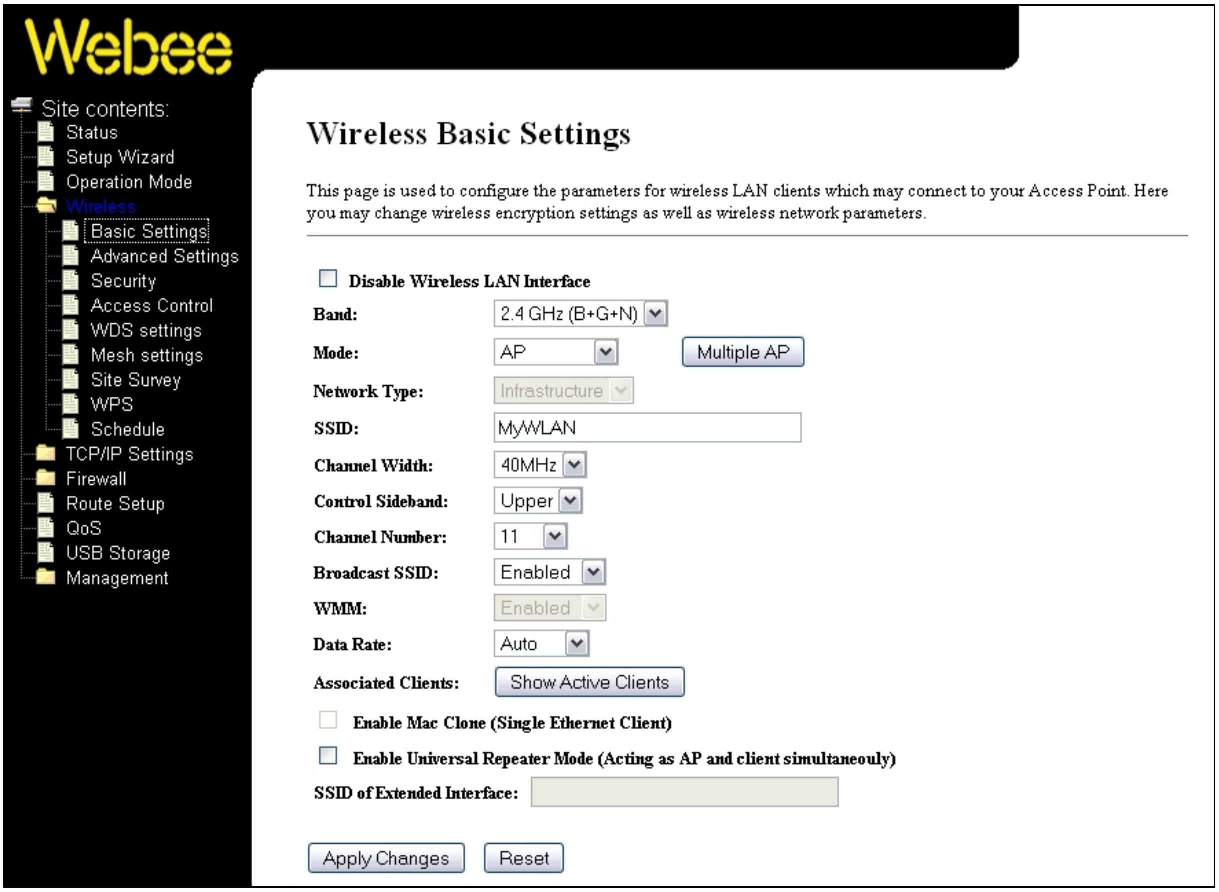
4. WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Wireless Basic Settings

This page is used to configure basic wireless parameters like Band, Mode, Network Type SSID, Channel Number, Enable Mac Clone (Single Ethernet Client)



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP [Multiple AP]
Network Type:	Infrastructure
SSID:	MyWLAN
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	[Show Active Clients]

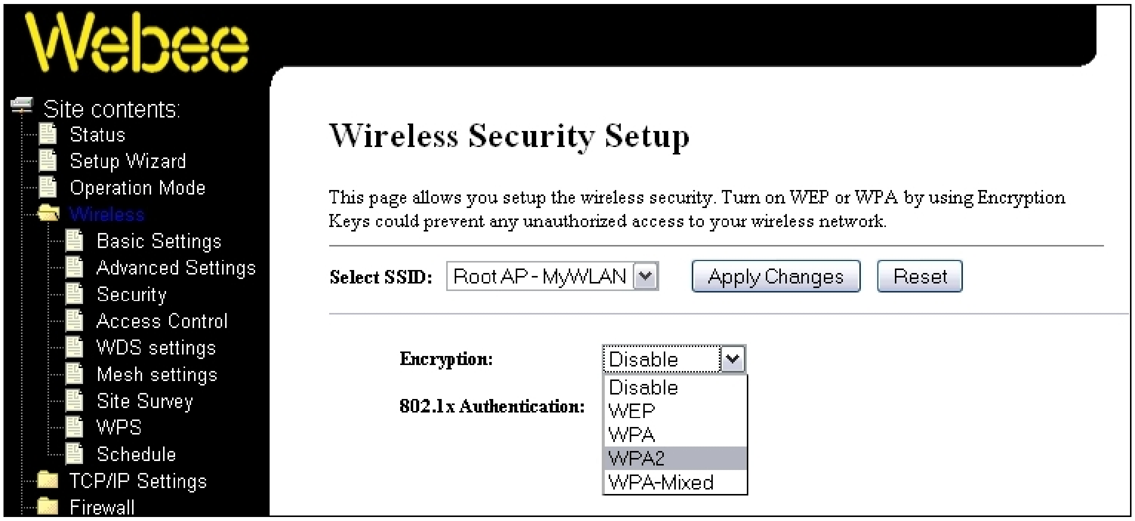
☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Wireless Security Setup

This page is used to configure wireless security



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

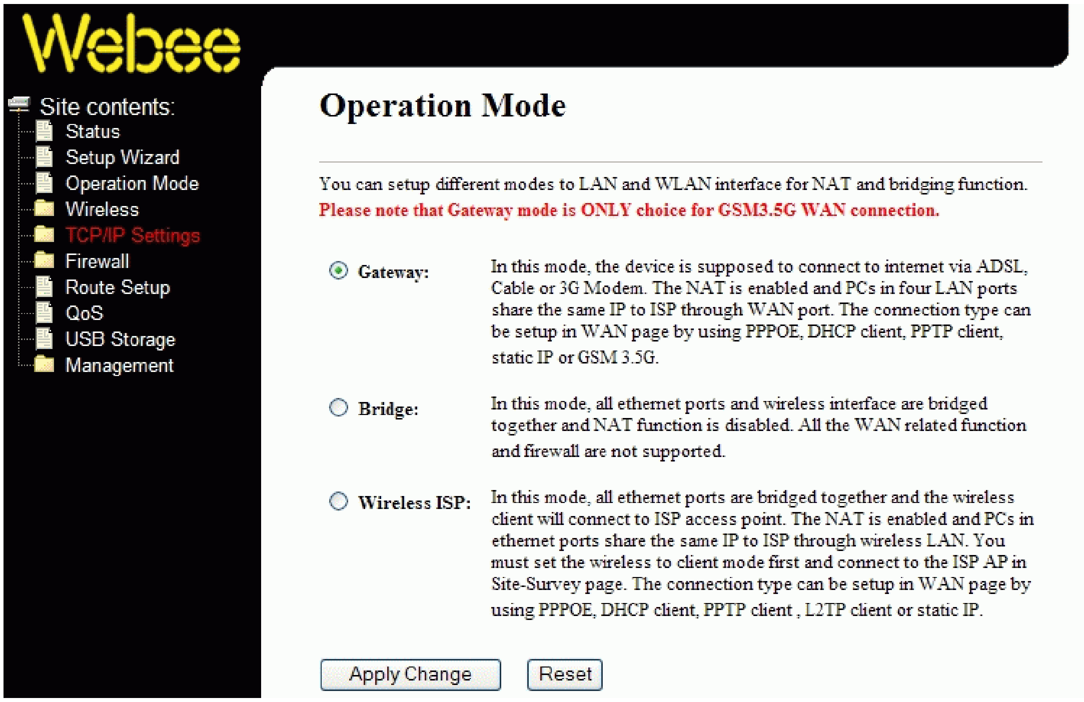
Select SSID: Root AP - MyWLAN

Encryption: Disable

802.1x Authentication:

4.3.3 Operation Mode

This page is used to configure in which mode the Router acts



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.
Please note that Gateway mode is ONLY choice for GSM3.5G WAN connection.

● **Gateway:** In this mode, the device is supposed to connect to internet via ADSL, Cable or 3G Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, static IP or GSM 3.5G.

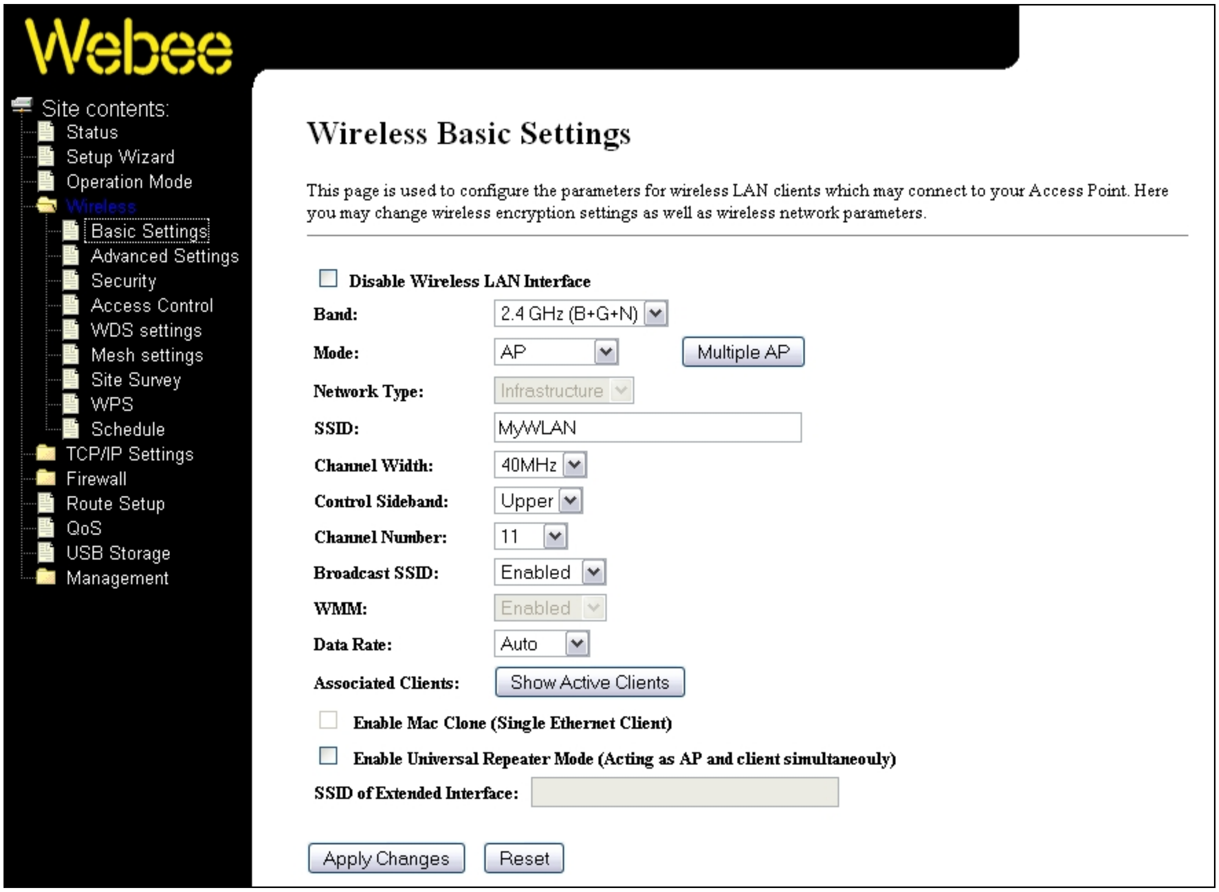
○ **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client , L2TP client or static IP.

Item	Description
Gateway	Traditional gateway configuration. It always connects internet via ADSL/Cable Modem. LAN interface, WAN interface, Wireless interface, NAT and Firewall modules are applied to this mode
Bridge	Each interface (LAN, WAN and Wireless) regards as bridge. NAT, Firewall and all router’s functions are not supported
Wireless ISP	Switch Wireless interface to WAN port and all Ethernet ports in bridge mode. Wireless interface can do all router’s functions
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.4 Wireless - Basic Settings

This page is used to configure the parameters for wireless LAN clients that may connect to your Webee Router. Here you may change wireless encryption settings as well as wireless network parameters.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	MyWLAN
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

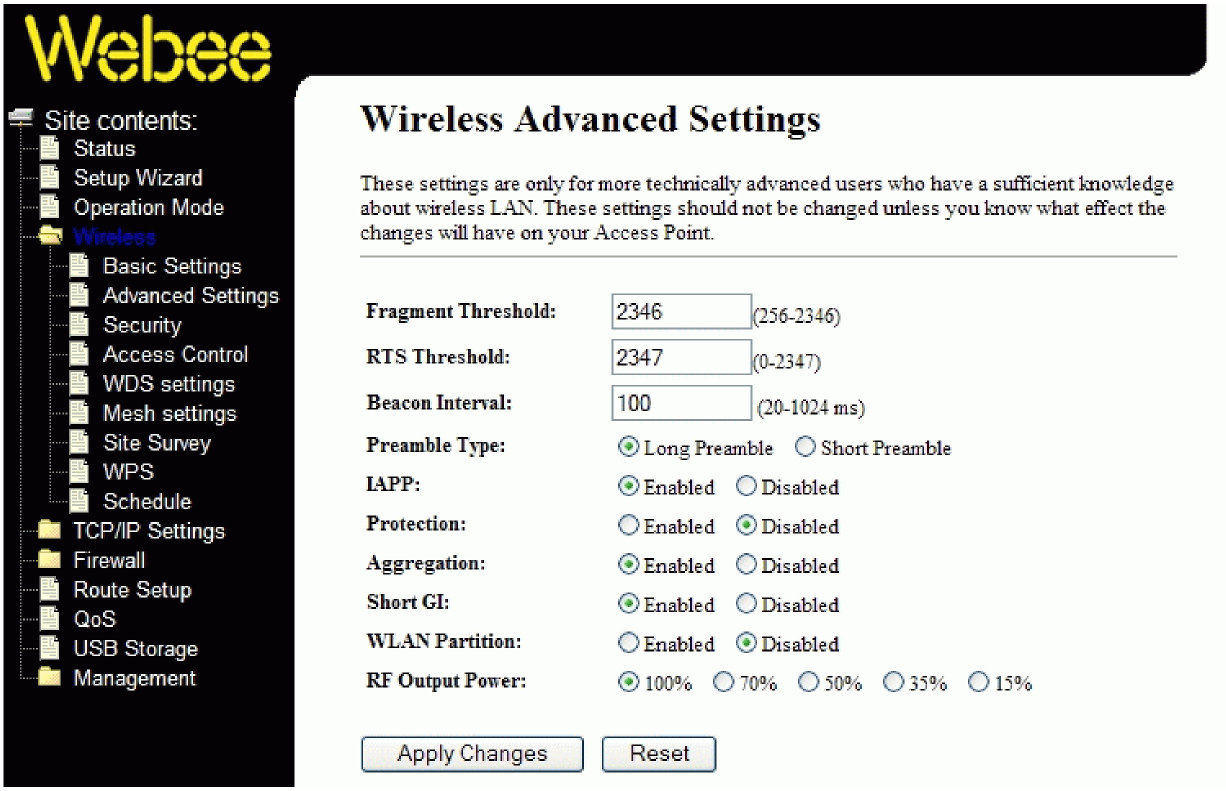
SSID of Extended Interface:

Item	Description
Disable Wireless LAN Interface	Click on to disable the wireless LAN data transmission.
Band	Click to select 2.4GHz(B) / 2.4GHz(G) / 2.4GHz(N) 2.4GHz(B+G)/ 2.4GHz(G+N) / 2.4GHz(B+G+N)
Mode	Click to select the WLAN AP / Client / WDS / AP+WDS wireless mode.
Network Type	While ***Mode*** is selected to be **Client**. Click to select the network type infrastructure or Ad hoc.
SSID	It is the wireless network name. The SSID can be 32 bytes long.
Channel Width	Select the operating channel width 20 MHz or 40 MHz. **[N band only]**
Control Sideband	Select the Sideband with Upper or Lower for channel width 40MHz. **[N band only]**
Channel Number	Select the wireless communication channel from pull-down menu.
Broadcast SSID	Click to enable or disable the SSID broadcast function. Refer to 4.14 What is SSID Broadcast?
WMM	Click Enabled/Disable*d* to init WMM feature.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS. Refer to 4.32 What is Modulation Coding Schemes (MCS)?
Associated Clients	Click the ***Show Active Clients*** button to open Active Wireless Client Table that shows the MAC address, transmit-packet, receive-packet

	and transmission-rate for each associated wireless client.
Enable Mac Clone (Single Ethernet Client)	Take Laptop NIC MAC address as wireless client MAC address. **[Client Mode only]**
Enable Universal Repeater Mode	Click to enable Universal Repeater Mode
SSID of Extended Interface	Assign SSID when enables Universal Repeater Mode.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.5 Wireless - Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Webee Router.



Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

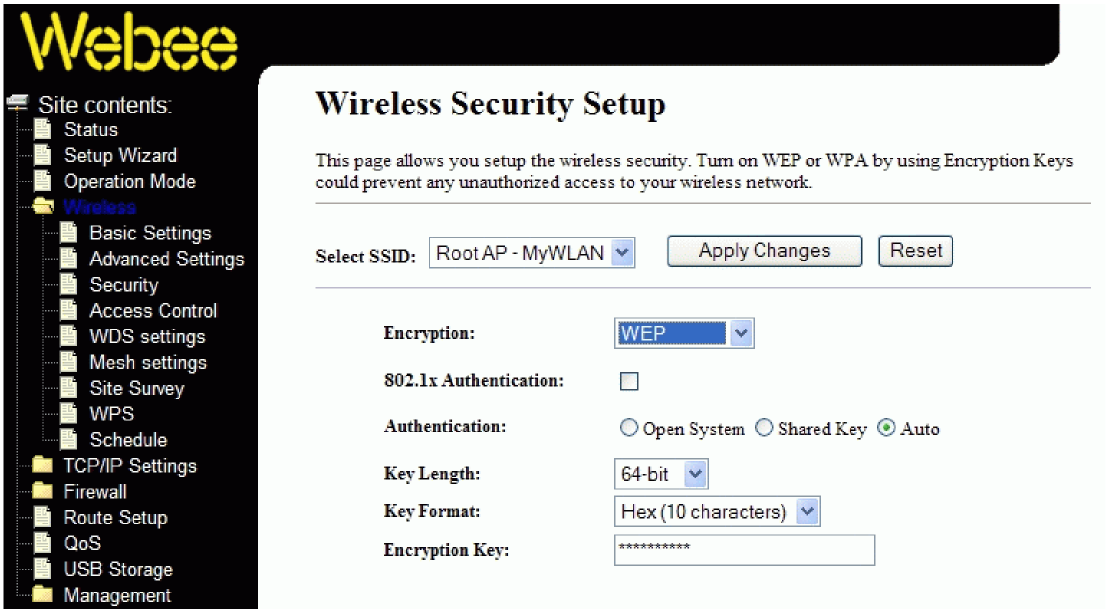
Fragment Threshold: 2346 (256-2346)
RTS Threshold: 2347 (0-2347)
Beacon Interval: 100 (20-1024 ms)
Preamble Type: ● Long Preamble ○ Short Preamble
IAPP: ● Enabled ○ Disabled
Protection: ○ Enabled ● Disabled
Aggregation: ● Enabled ○ Disabled
Short GI: ● Enabled ○ Disabled
WLAN Partition: ○ Enabled ● Disabled
RF Output Power: ● 100% ○ 70% ○ 50% ○ 35% ○ 15%

Item	Description
Fragment Threshold	Set the data packet fragmentation threshold, value can be written between 256 and 2346 bytes. Refer to 4.10 What is Fragment Threshold?
RTS Threshold	Set the RTS Threshold, value can be written between 0 and 2347 bytes. Refer to 4.11 What is RTS(Request To Send) Threshold?

Beacon Interval	Set the Beacon Interval, value can be written between 20 and 1024 ms. Refer to 4.12 What is Beacon Interval?
Preamble Type	Click to select the ***Long Preamble*** or ***Short Preamble*** support on the wireless data packet transmission. Refer to 4.13 What is Preamble Type?
IAPP	Click to enable or disable the IAPP function. Refer to 4.20 What is Inter-Access Point Protocol(IAPP)?
Protection	Protect 802.11n user priority.
Aggregation	Click to enable or disable the Aggregation function. Refer to 4.33 What is Aggregation?
Short GI	Click to enable or disable the short Guard Intervals function. Refer to 4.34 What is Guard Intervals (GI)?
RF Output Power	To adjust transmission power level.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.6 Wireless - Security Setup

This page allows you setup the wireless security. Turn on WEP, WPA, WPA2 by using encryption keys could prevent any unauthorized access to your wireless network.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - MyWLAN

Encryption: WEP

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: **********

Item	Description
Select SSID	Select the SSID from multiple APs.
Encryption	Select the encryption supported over wireless access. The encryption method can be None, WEP, WPA, WPA2 or WPA-Mixed Refer to 4.9 What is WEP? 4.15 What is Wi-Fi Protected Access (WPA)?

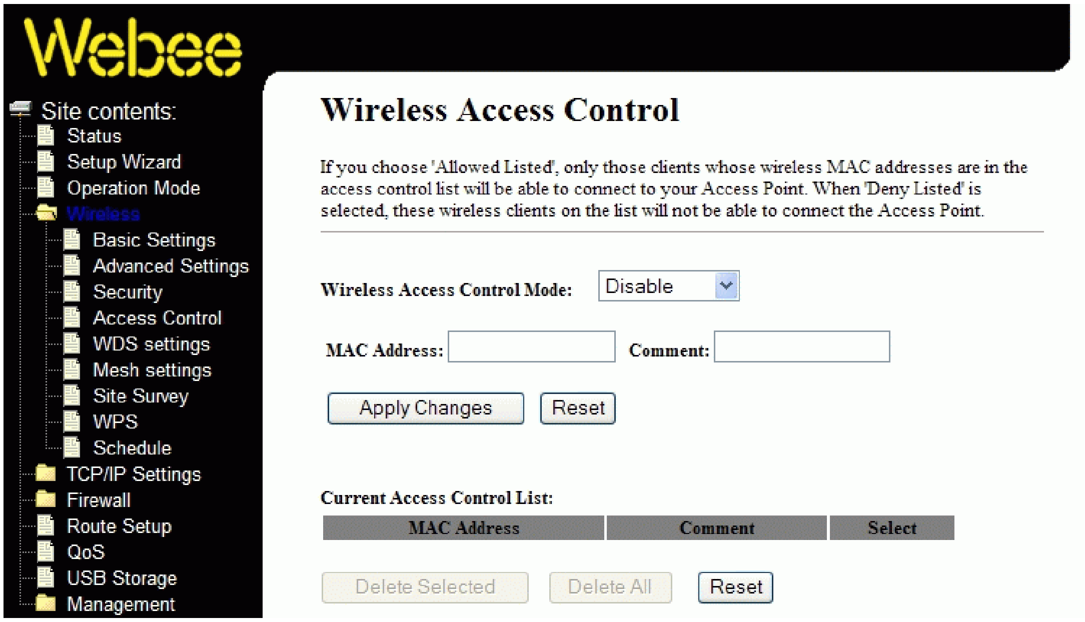
	4.16 What is WPA2?
Use 802.1x Authentication	While Encryption is selected to be WEP. Click the check box to enable IEEE 802.1x authentication function. Refer to 4.17 What is 802.1x Authentication?
Authentication Type	Click to select the authentication type in ***Open System***, ***Shared Key*** or ***Auto*** selection.
Key Length	Select the WEP shared secret key length from pull-down menu. The length can be chose between 64-bit and 128-bit (known as "WEP2") keys. The WEP key is composed of initialization vector (24 bits) and secret key (40-bit or 104-bit).
Key Format	Select the WEP shared secret key format from pull-down menu. The format can be chose between plant text (ASCII) and hexadecimal (HEX) code.
Encryption Key	Secret key of WEP security encryption function.
WPA Authentication Mode	While Encryption is selected to be WPA. Click to select the WPA Authentication Mode with Enterprise (RADIUS) or Personal (Pre-Shared Key). Refer to 4.15 What is Wi-Fi Protected Access (WPA)?
WPA Cipher Suite	Select the Cipher Suite for WPA encryption. 4.18 What is Temporal Key Integrity Protocol (TKIP)? 4.19 What is Advanced Encryption Standard (AES)?
WPA2 Cipher Suite	Select the Cipher Suite for WPA2 encryption.
Pre-Shared Key Format	While Encryption is selected to be WPA. Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters). **[WPA, Personal(Pre-Shared Key) only]**
Pre-Shared Key	Fill in the key value. [WPA, Personal(Pre-Shared Key) only]
Enable Pre-Authentication	Click to enable Pre-Authentication. [WPA2/WPA2 Mixed only, Enterprise only]
Authentication RADIUS Server	Set the IP address, port and login password information of authentication RADIUS sever.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

WEP encryption key (secret key) length:

Length / Format	64-bit	128-bit
ASCII	5 characters	13 characters
HEX	10 hexadecimal codes	26 hexadecimal codes

4.3.7 Wireless - Access Control

If you enable wireless access control, only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When this option is enabled, no wireless clients will be able to connect if the list contains no entries.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

MAC Address: Comment:

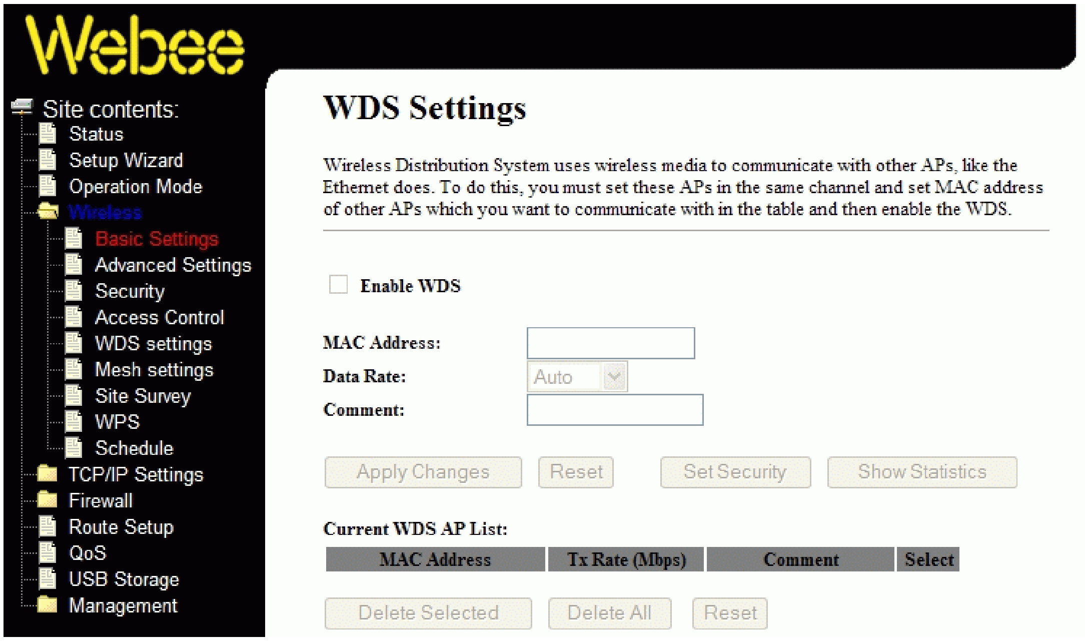
Current Access Control List:

MAC Address	Comment	Select

Item	Description
Wireless Access Control Mode	Click the ***Disabled***, ***Allow Listed*** or ***Deny Listed*** of drop down menu choose wireless access control mode. This is a security control function; only those clients registered in the access control list can link to this Webee Router.
MAC Address	Fill in the MAC address of client to register this Webee Router access capability.
Comment	Fill in the comment tag for the registered client.
Apply Changes	Click the ***Apply Changes*** button to register the client to new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Current Access Control List	It shows the registered clients that are allowed to link to this Webee Router.
Delete Selected	Click to delete the selected clients that will be access right removed from this Webee Router.
Delete All	Click to delete all the registered clients from the access allowed list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.8 WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other AP that you want to communicate with in the table and then enable the WDS.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☐ Enable WDS

MAC Address:

Data Rate: Auto

Comment:

Current WDS AP List:

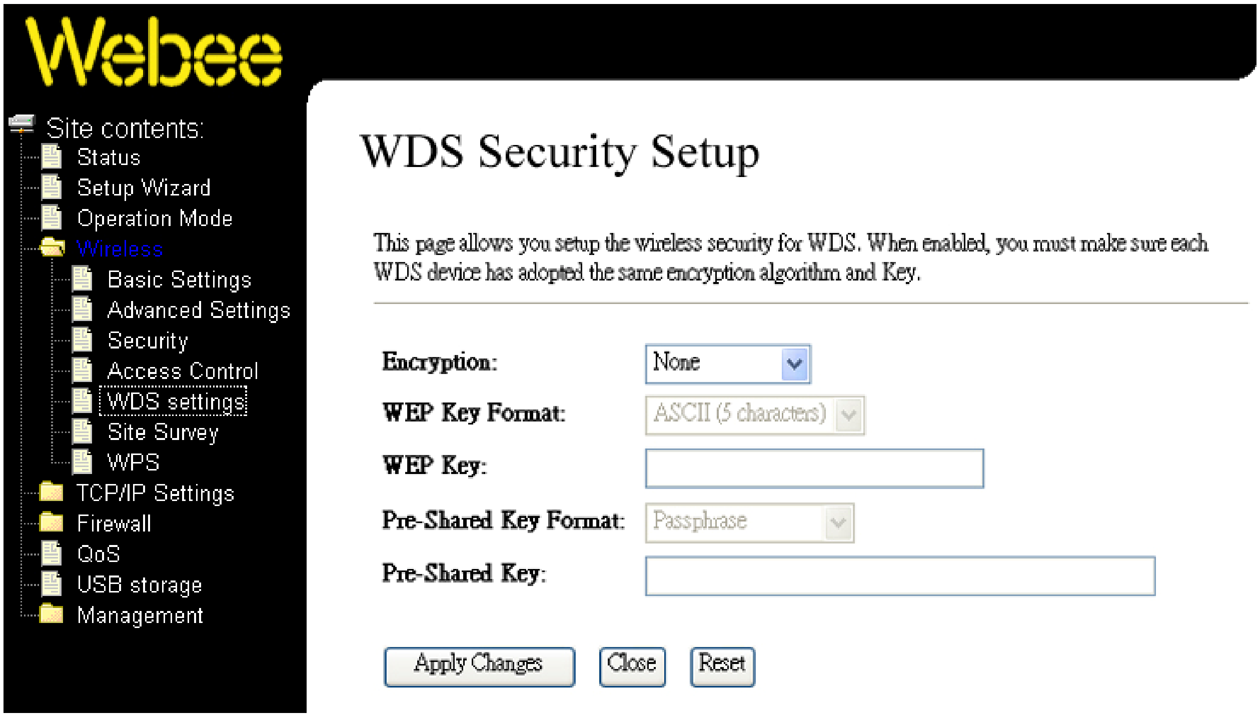
MAC Address	Tx Rate (Mbps)	Comment	Select

Item	Description
Enable WDS	Click the check box to enable wireless distribution system. Refer to 4.21 What is Wireless Distribution System (WDS)?
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Data Rate	Select the transmission data rate from pull-down menu. Data rate can be auto-select, 1M to 54Mbps or MCS.
Comment	Fill in the comment tag for the registered AP.
Apply Changes	Click the ***Apply Changes*** button to register the AP to new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Set Security	Click button to configure wireless security like ***WEP(64bits), WEP(128bits), WPA(TKIP), WPA2(AES)*** or ***None***
Show Statistics	It shows the TX, RX packets, rate statistics
Delete Selected	Click to delete the selected clients that will be removed from the wireless distribution system.
Delete All	Click to delete all the registered APs from the wireless distribution system allowed list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

WDS Security Setup

Requirement: Set [Wireless]->[Basic Settings]->[Mode]->AP+WDS

This page is used to configure the wireless security between APs. Refer to 3.3.6 Wireless Security Setup.



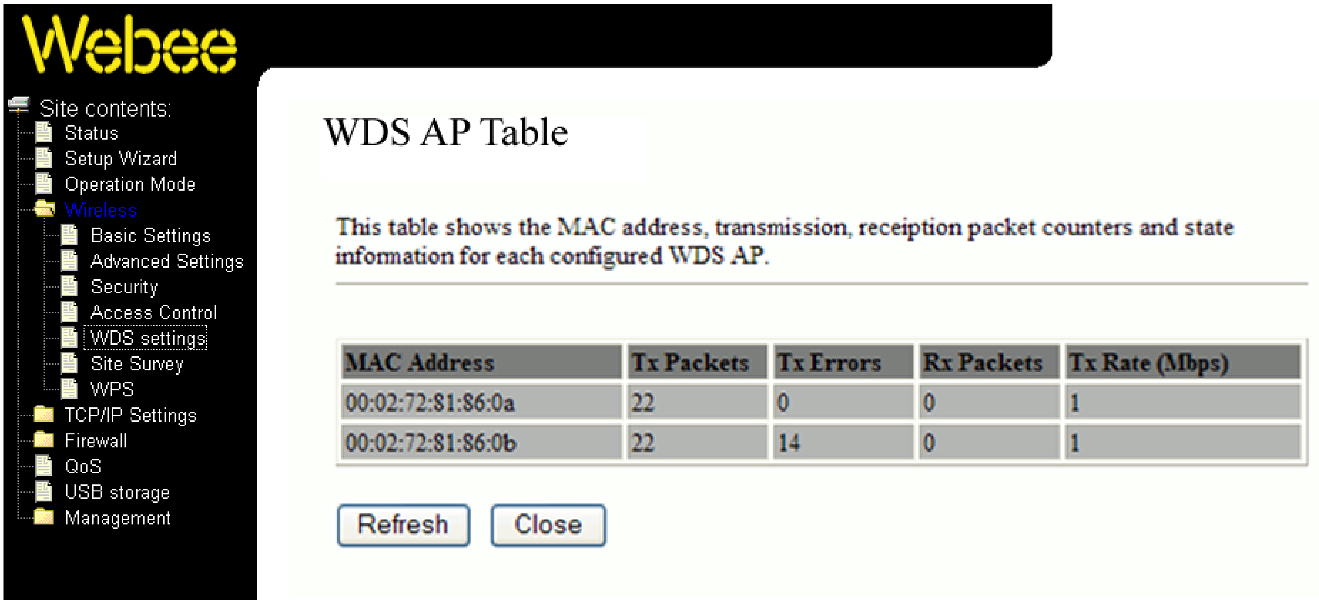
WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	None
WEP Key Format:	ASCII (5 characters)
WEP Key:	
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

WDS AP Table

This page is used to show WDS statistics



WDS AP Table

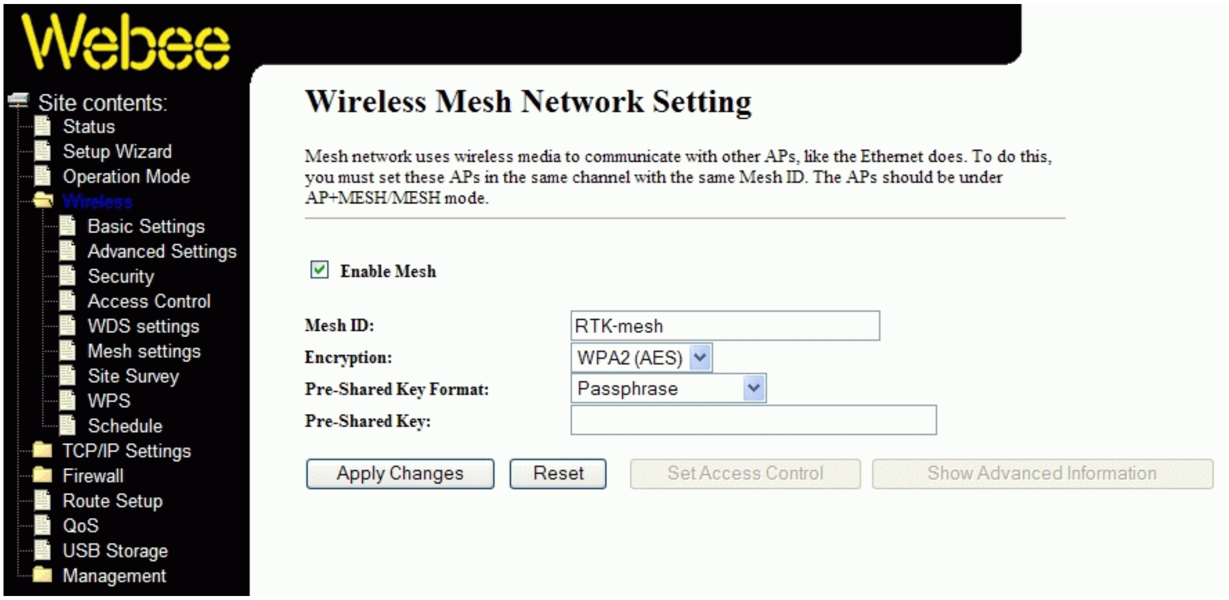
This table shows the MAC address, transmission, receiption packet counters and state information for each configured WDS AP.

MAC Address	Tx Packets	Tx Errors	Rx Packets	Tx Rate (Mbps)
00:02:72:81:86:0a	22	0	0	1
00:02:72:81:86:0b	22	14	0	1

Item	Description
MAC Address	It shows the MAC Address within WDS.
Tx Packets	It shows the statistic count of sent packets on the wireless LAN interface.
Tx Errors	It shows the statistic count of error sent packets on the Wireless LAN interface.
Rx Packets	It shows the statistic count of received packets on the wireless LAN interface.
Tx Rare (Mbps)	It shows the wireless link rate within WDS.
Refresh	Click to refresh the statistic counters on the screen.
Close	Click to close the current window.

4.3.9 Mesh Settings

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set the APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.



Wireless Mesh Network Setting

Mesh network uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel with the same Mesh ID. The APs should be under AP+MESH/MESH mode.

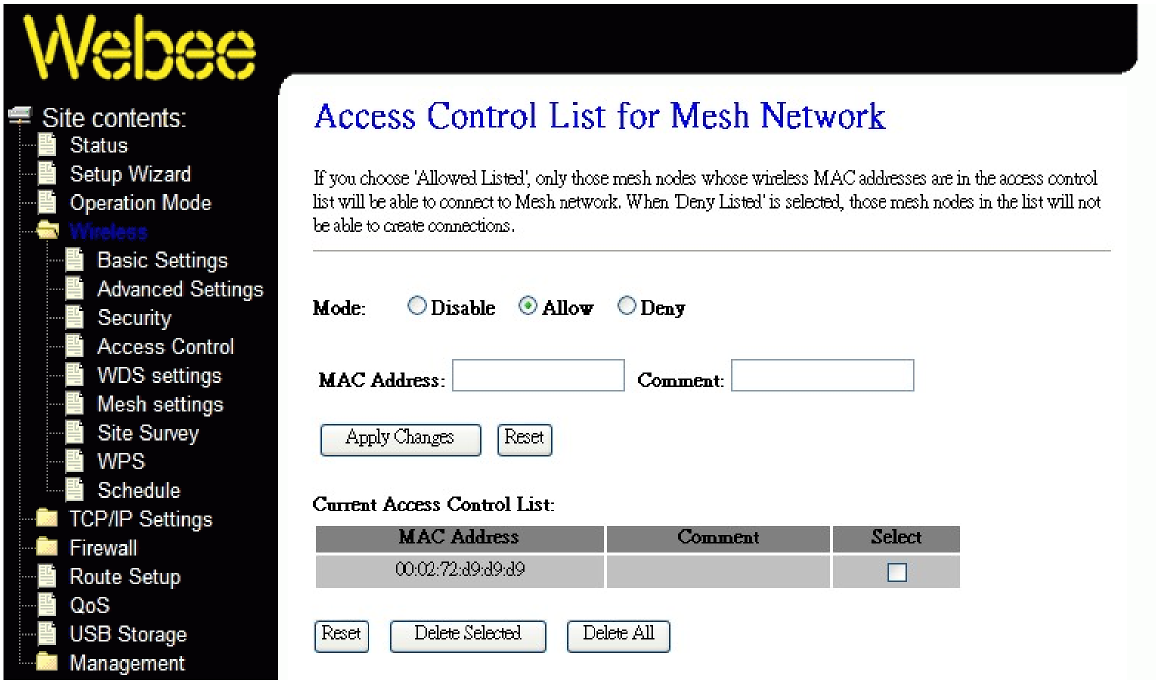
☑ **Enable Mesh**

Mesh ID: RTK-mesh
Encryption: WPA2 (AES)
Pre-Shared Key Format: Passphrase
Pre-Shared Key:

Item	Description
Enable Mesh	Click Checkbox to enable wireless Mesh function
Mesh ID	It is the wireless Mesh name. The SSID can be 32 bytes long.
Encryption	Select the encryption supported over wireless access. The encryption method can be None or WPA2(AES)
Pre-Shared Key Formate	Select the Pre-shared key format from the pull-down menu. The format can be Passphrase or Hex (64 characters).
Pre-Shared Key	Fill in the key value.
Apply Changes	Click the ***Apply Changes*** button to register the AP to new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Set Access Control	It is only used for advanced users to setup the access control rules of MPs. When click the “Set Access Control” button, the “Access Control List for Mesh Network” page is presented.
Show Advanced Information	Advanced users could click the “Show Advanced Information” button to access the “Wireless Mesh Network Information” page for detailed information of current mesh network.

Access Control List for Mesh Network

If you choose ‘Allowed Listed’, only those mesh nodes whose wireless MAC addresses are in the access control list will be able to connect to Mesh network. When ‘Deny Listed’ is selected, those mesh nodes in thelist will not be able to create connections.



Access Control List for Mesh Network

If you choose 'Allowed Listed', only those mesh nodes whose wireless MAC addresses are in the access control list will be able to connect to Mesh network. When 'Deny Listed' is selected, those mesh nodes in the list will not be able to create connections.

Mode: ○ Disable ● Allow ○ Deny

MAC Address: ______ Comment: ______

[Apply Changes] [Reset]

Current Access Control List:

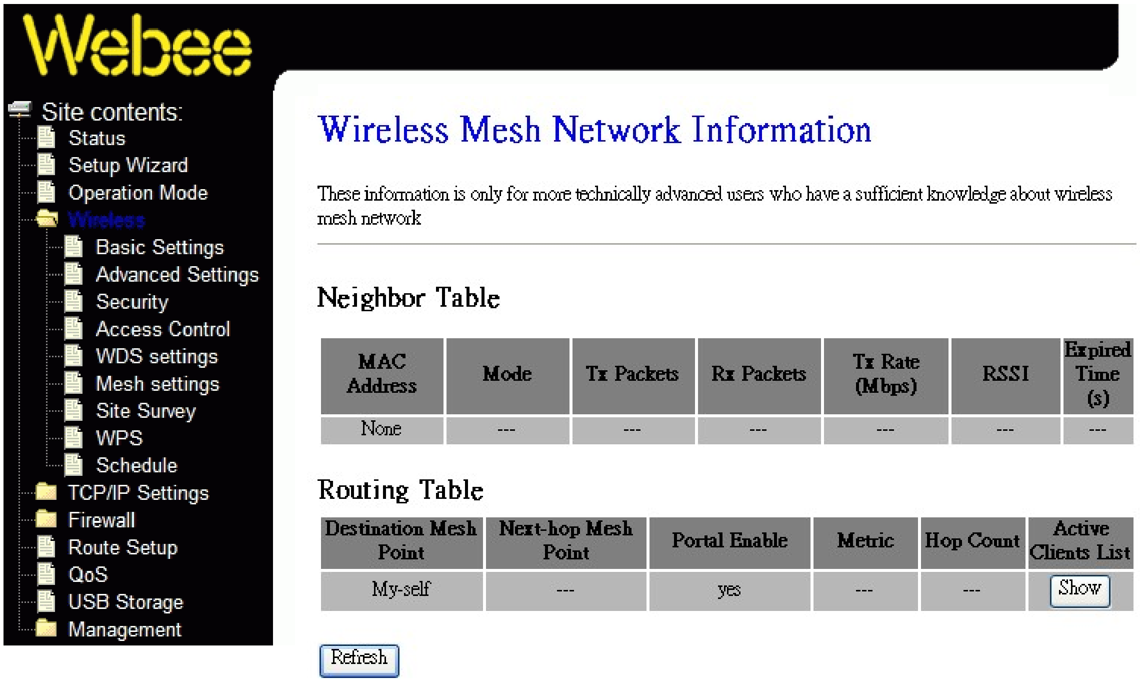
MAC Address	Comment	Select
00:02:72:d9:d9:d9		□

[Reset] [Delete Selected] [Delete All]

Item	Description
Mode :	Click the radio button to select Disable, Allow or Deny the List.
MAC Address	Fill in the MAC address of AP to register the wireless distribution system access capability.
Comment	Fill in the comment tag for the registered AP.
Apply Changes	Whenever users change setting or add rules to the ACL, they need to apply this button to commit changes.
Reset	It restores the original values of “Mode” and cleans the text fields of “MAC Address” and “Comment”.
Delete Selected	Click to delete the selected MAC address that will be removed from the list
Delete All	Click to delete all the registered entries from the list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

Wireless Mesh Network Information

These information is only for more technically advanced users who have a sufficient knowledge about wireless mesh network.



Wireless Mesh Network Information

These information is only for more technically advanced users who have a sufficient knowledge about wireless mesh network

Neighbor Table

MAC Address	Mode	Tx Packets	Rx Packets	Tx Rate (Mbps)	RSSI	Expired Time (s)
None	---	---	---	---	---	---

Routing Table

Destination Mesh Point	Next-hop Mesh Point	Portal Enable	Metric	Hop Count	Active Clients List
My-self	---	yes	---	---	Show

Neighbor Table

The “Neighbor Table” lists the neighbor MPs and Their statistics. Explannation of each column is listed as follows:

Item	Description
MAC Address	MAC address of the neighbor MP
Mode	Mode of current connection with the neighbor MP, eg. 11n/11g/11b.
Tx Packets	Number of transmitted packets to the neighbor MP
Rx Packets	Number of received packets from the neighbor MP
Tx Rate (Mbps)	Transmission data rate
RSSI	Signal quality used for mesh metric
Expire time	Expire time of the mesh neighborhood

Routing Table

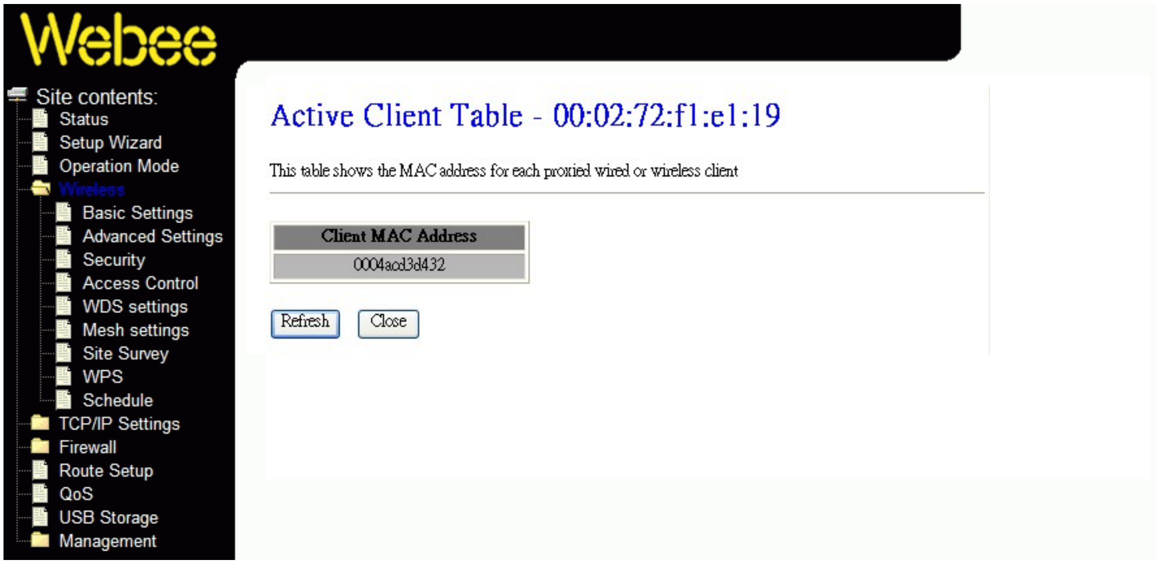
The “Routing Table” lists the routing information learned by the MP. Explanation of each column is listed as follows:

Item	Description
Next hop Mesh Point	The address of the neighbor MP to that data packet for the destination should be forwarded.
Portal Enable	This column shows if the destination MP is a portal or not.

Metric	Cumulative metric from this MP to the destination using this route.
Hop Count	Number of hops to the destination MP.
Active Clients List	Clicking the button to pop up a “Active Client Table” page that shows the active wired or wireless clients proxied by the destination MP.

Active Client Table

This table shows the MAC address for each proxied wired or wireless client.



Active Client Table - 00:02:72:f1:e1:19

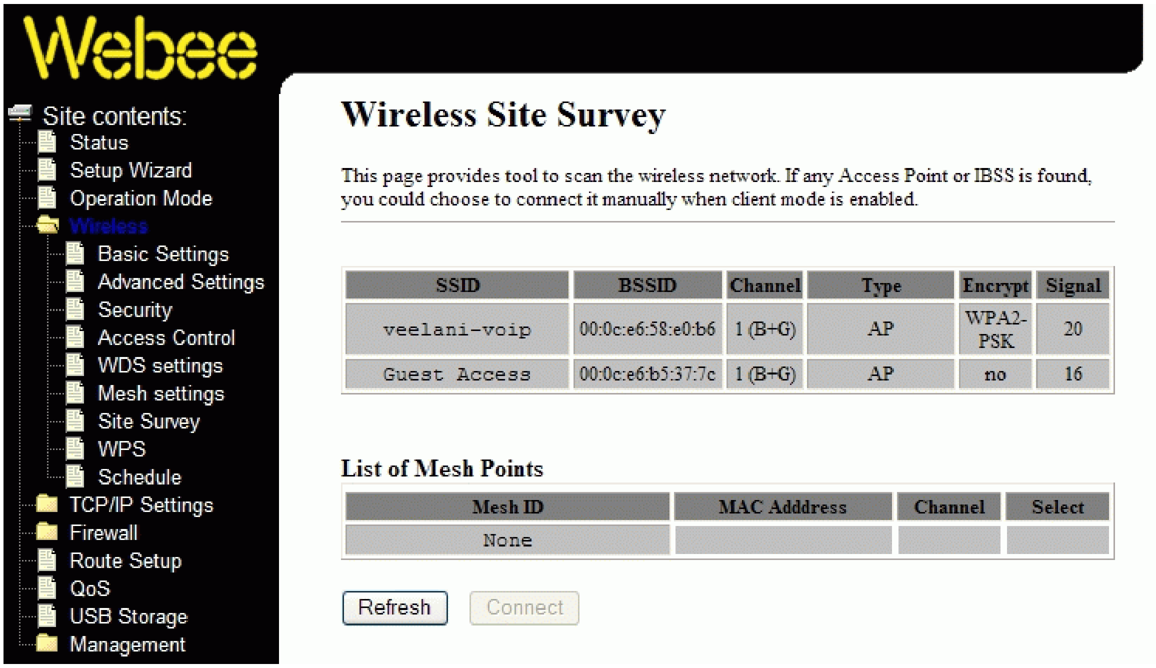
This table shows the MAC address for each proxied wired or wireless client

Client MAC Address
0004acd3d432

Item	Description
Refresh	Click ***Refresh*** button can refresh the current information shown in this page.
Close	Click ***Close*** button can close the popped-up window.

4.3.10 Site Survey

This page is used to view or configure other APs near yours.



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal
veelani-voip	00:0c:e6:58:e0:b6	1 (B+G)	AP	WPA2-PSK	20
Guest Access	00:0c:e6:b5:37:7c	1 (B+G)	AP	no	16

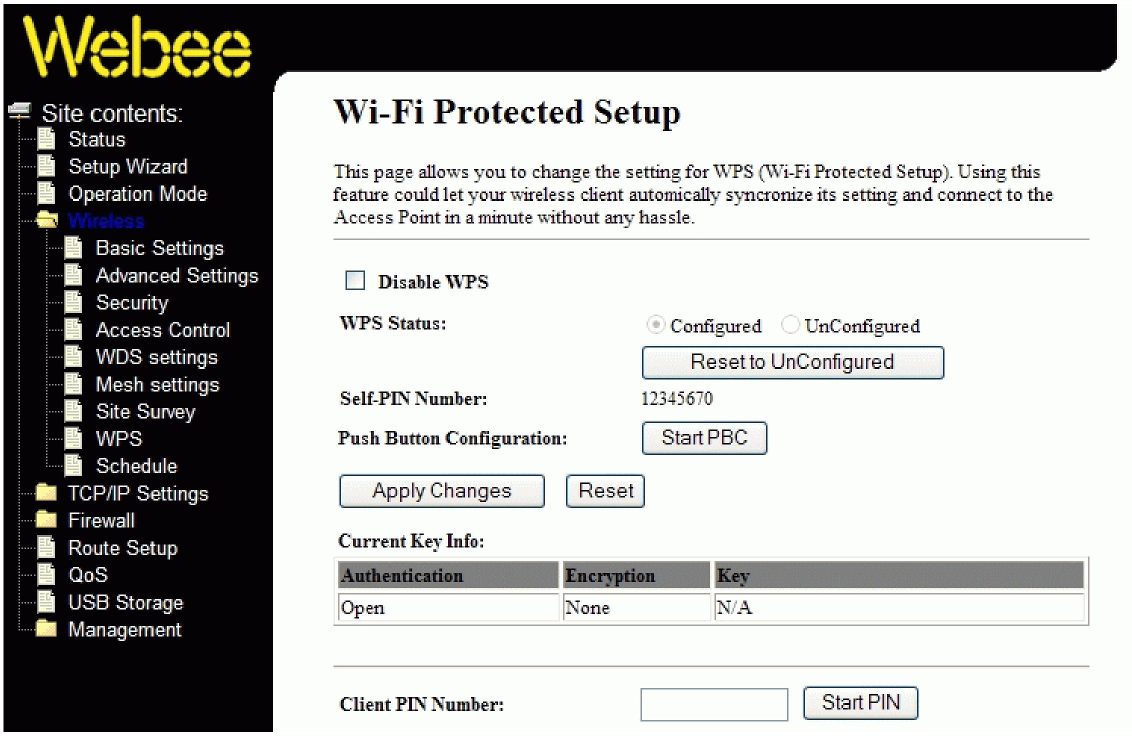
List of Mesh Points

Mesh ID	MAC Adddress	Channel	Select
None			

Item	Description
SSID	It shows the SSID of AP.
BSSID	It shows BSSID of AP.
Channel	It show the current channel of AP occupied.
Type	It show which type AP acts.
Encrypt	It shows the encryption status.
Signal	It shows the power level of current AP.
Select	Click to select AP or client you'd like to connect.
Refresh	Click the ***Refresh*** button to re-scan site survey on the screen.
Connect	Click the ***Connect*** button to establish connection.

4.3.11 WPS

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

□ **Disable WPS**

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 12345670

Push Button Configuration:

Current Key Info:

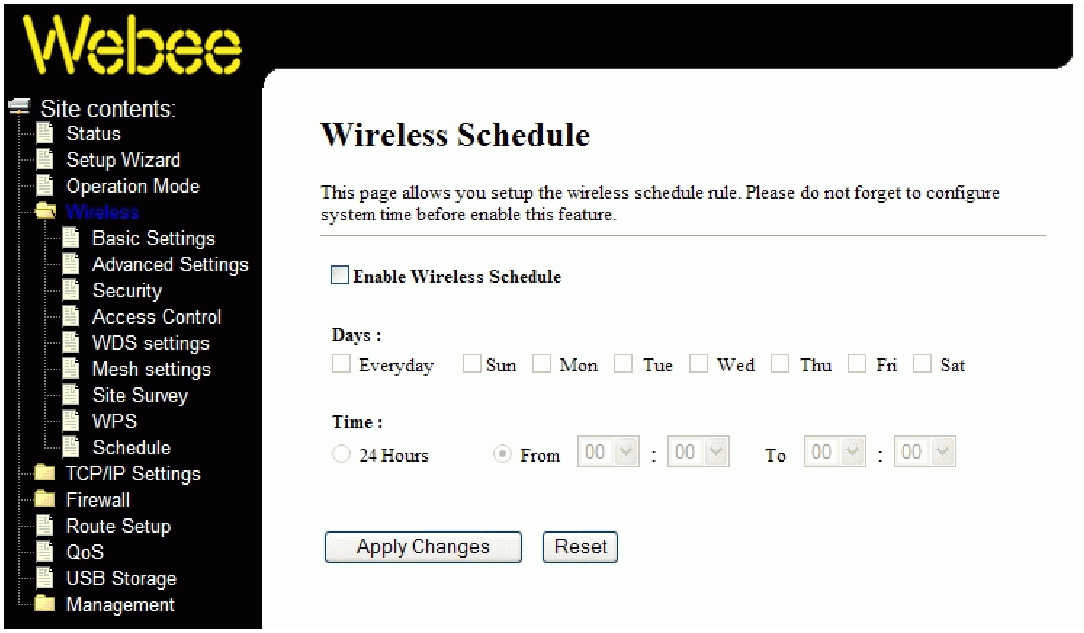
Authentication	Encryption	Key
Open	None	N/A

Client PIN Number:

Item	Description
Disable WPS	Click on to disable the Wi-Fi Protected Setup function.
WPS Status	Show WPS status is ***Configured*** or ***UnConfigured***.
Self-PIN Number	Fill in the PIN Number of AP to register the wireless distribution system access capability.
Push Button Configuration	The ***Start PBC*** button provides tool to scan the wireless network. If any Access Point or IBSS is found, you could connect it automatically when client join PBC mode.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Current Key Info	**Authentication**□It shows the Authentication is opened or closed. **Encryption**□It shows the Encryption mode. **Key**□It shows the Encryption key.
Client PIN Number	Fill in the ***Client PIN Number*** from your Client sites.

4.3.12 Schedule

This page is to configure the wireless activation timestamp by users.



Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

☐ **Enable Wireless Schedule**

Days :

☐ Everyday ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

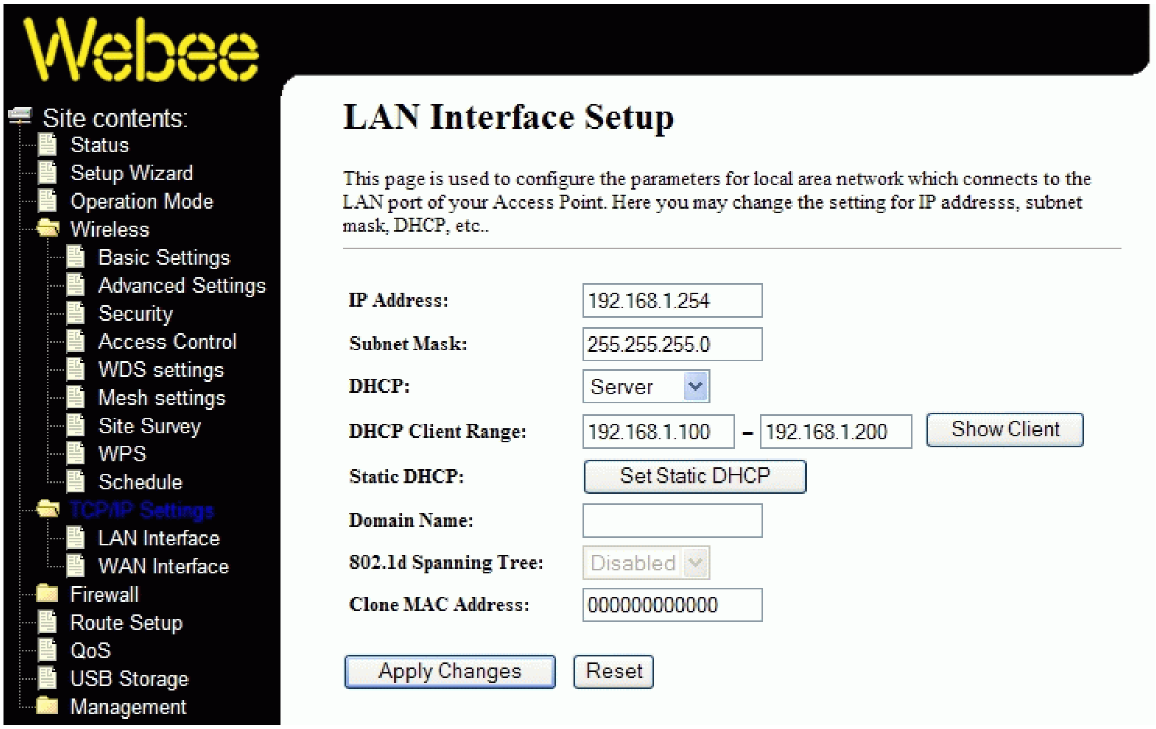
Time :

○ 24 Hours ● From 00 : 00 To 00 : 00

Item	Description
Enable Wireless Schedule	Click on to enable the wireless schedule function.
Days	Click the one or more of days to set the rules.
Time	Click 24 hrs or set the starting time and ending time.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.13 LAN Interface Setup

This page is used to configure the parameters for local area network that connects to the LAN ports of your Webee Router. Here you may change the setting for IP address, subnet mask, DHCP, etc.



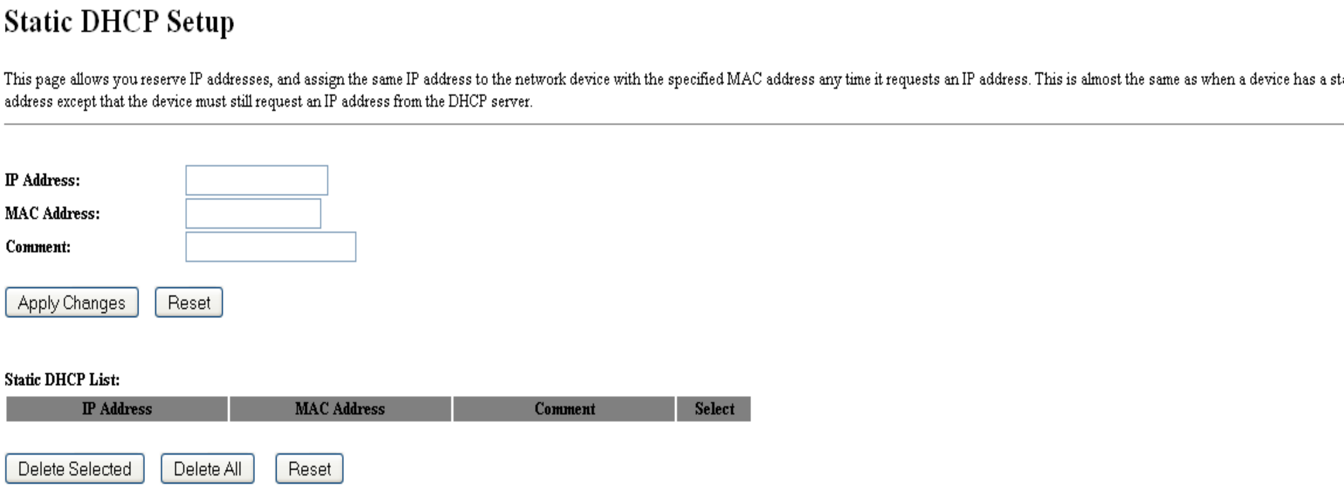
LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200 Show Client
Static DHCP:	Set Static DHCP
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Item	Description
IP Address	Fill in the IP address of LAN interfaces of this WLAN Access Point.
Subnet Mask	Fill in the subnet mask of LAN interfaces of this WLAN Access Point.
DHCP	Click to select ***Disabled***, ***Client*** or ***Server*** in different operation mode of wireless Access Point.
DHCP Client Range	Fill in the start IP address and end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Show Client	Click to open the ***Active DHCP Client Table*** window that shows the active clients with their assigned IP address, MAC address and time expired information. **[Server mode only]**
Static DHCP	Select enable or disable the Static DHCP function from pull-down menu. **[Server mode only]**
Set Static DHCP	Manual setup Static DHCP IP address for specific MAC address. **[Server mode only]**
Domain Name	Assign Domain Name and dispatch to DHCP clients. It is optional field.
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

Static DHCP Setup



Static DHCP Setup

This page allows you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a sta
address except that the device must still request an IP address from the DHCP server.

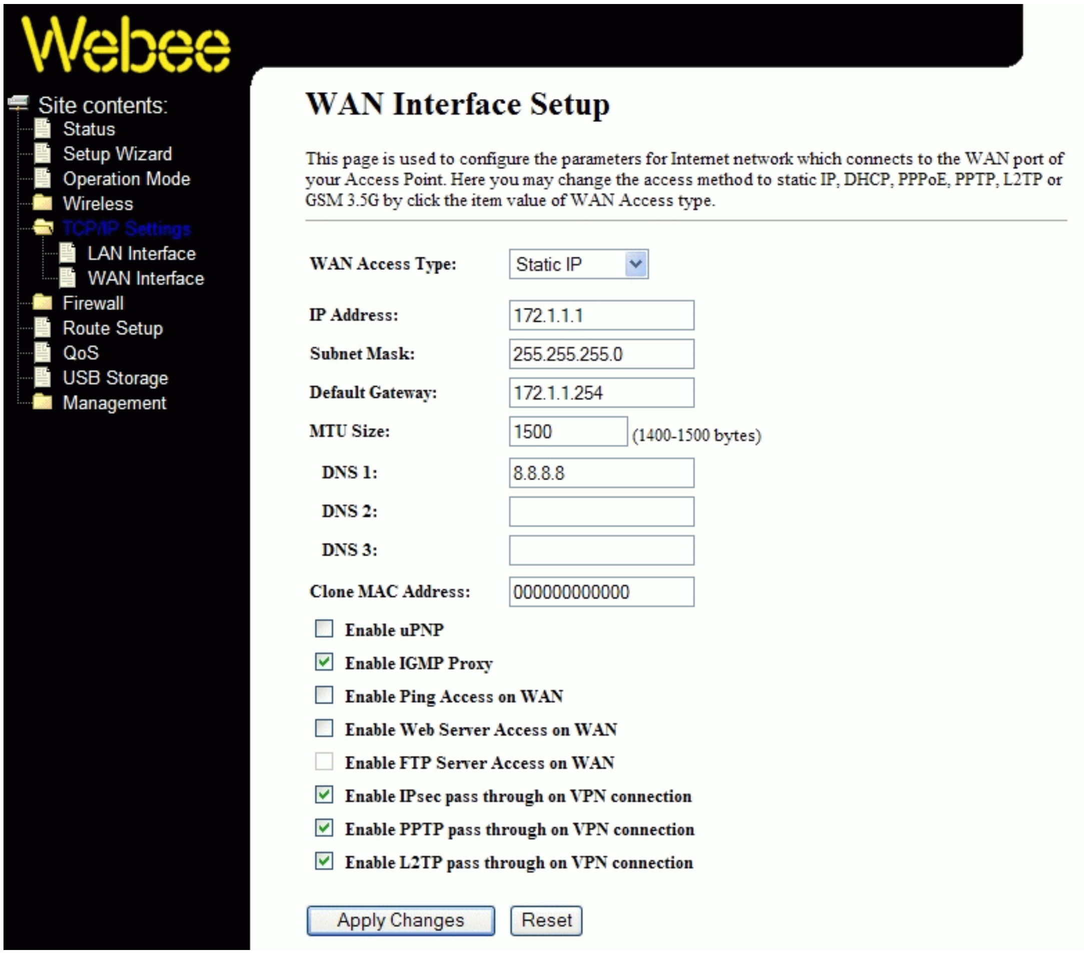
IP Address	MAC Address	Comment	Select

Item	Description
IP Address	If you select the Set Static DHCP on LAN interface, fill in the IP address for it.
MAC Address	If you select the Set Static DHCP on LAN interface, fill in the MAC address for it.
Comment	Fill in the comment tag for the registered Static DHCP.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Static DHCP List	It shows IP Address、MAC Address from the Static DHCP.
Delete Selected	Click to delete the selected clients that will be removed from the Static DHCP list.
Delete All	Click to delete all the registered clients from the Static DHCP list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.14 WAN Interface Setup

This page is used to configure the parameters for wide area network that connects to the WAN port of your Webee Router. Here you may change the access method to ***Static IP***, ***DHCP***, ***PPPoE*** , ***PPTP L2TP*** or ***GSM 3.5G*** by click the item value of **WAN Access Type**.

Static IP



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	8.8.8.8
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

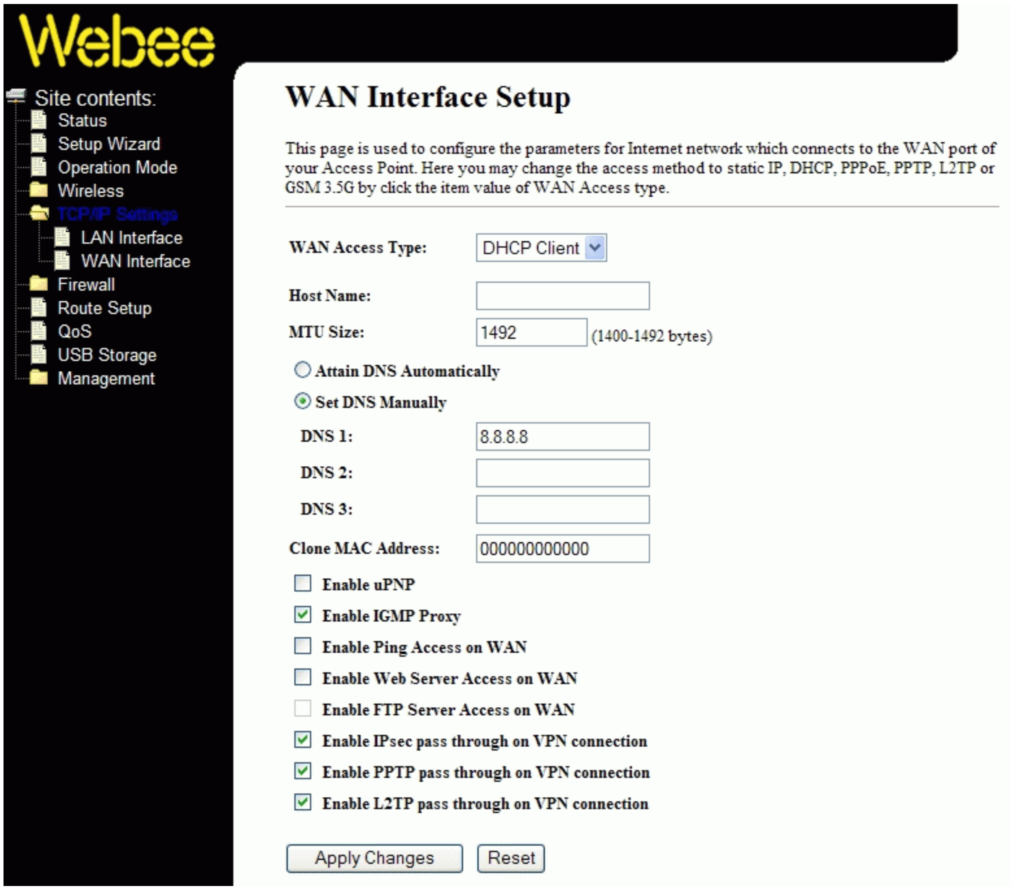
☐ **Enable uPNP**
☑ **Enable IGMP Proxy**
☐ **Enable Ping Access on WAN**
☐ **Enable Web Server Access on WAN**
☐ **Enable FTP Server Access on WAN**
☑ **Enable IPsec pass through on VPN connection**
☑ **Enable PPTP pass through on VPN connection**
☑ **Enable L2TP pass through on VPN connection**

Apply Changes | Reset

Item	Description
Static IP	Click to select Static IP support on WAN interface. There are IP address, subnet mask and default gateway settings need to be done.
IP Address	If you select the Static IP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the Static IP support on WAN interface, fill in the subnet mask for it.
Default Gateway	If you select the Static IP support on WAN interface, fill in the default gateway for WAN interface out going data packets.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1500
DNS 1	Fill in the IP address of Domain Name Server 1.

DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

DHCP Client



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1: 8.8.8.8

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

□ Enable FTP Server Access on WAN

☑ Enable IPsec pass through on VPN connection

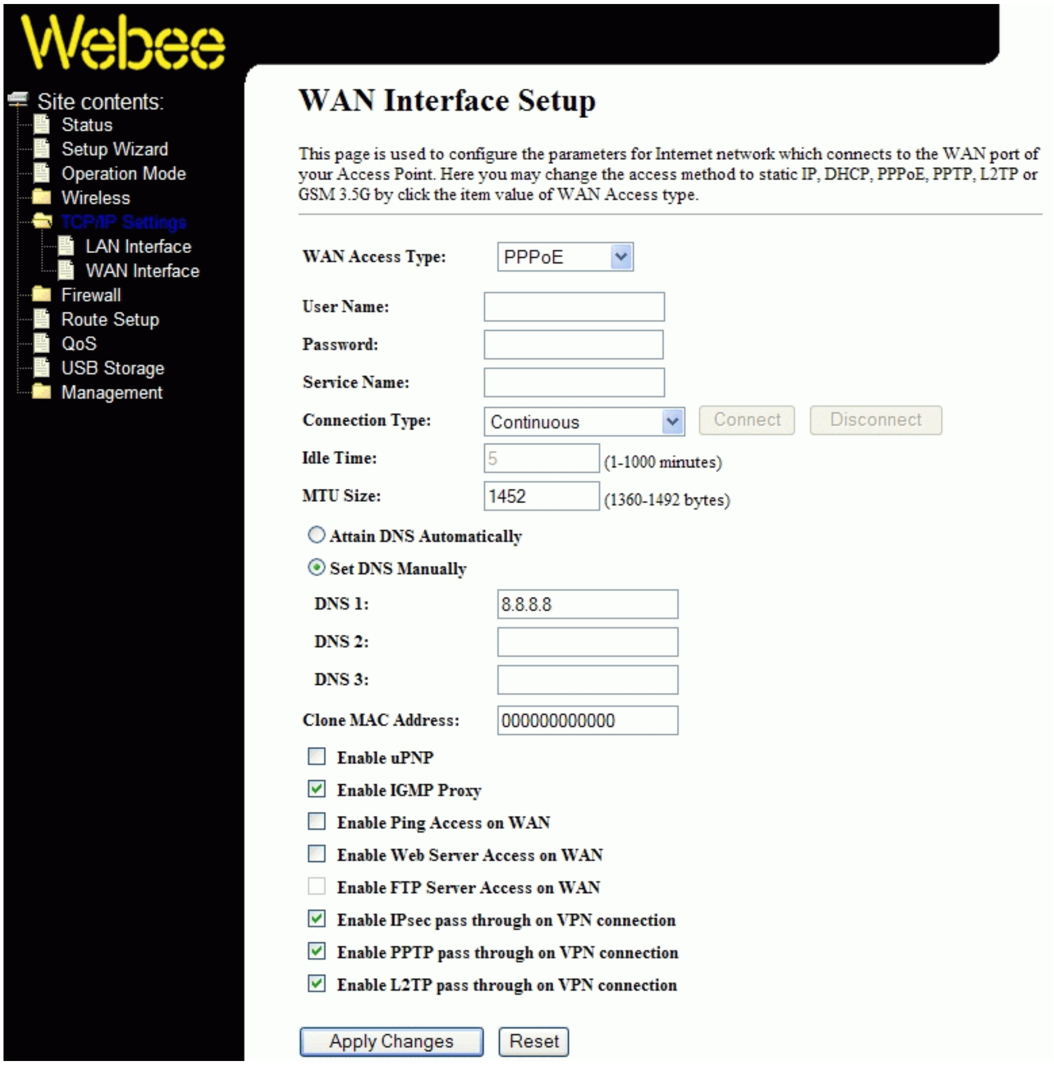
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

Item	Description
DHCP Client	Click to select DHCP support on WAN interface for IP address assigned automatically from a DHCP server.
Host Name	Fill in the host name of Host Name. The default value is empty
MTU Size	Fill in the mtu size of MTU Size. The default value is 1492
Attain DNS Automatically	Click to select getting DNS address for ***DHCP*** support. Please select ***Set DNS Manually*** if the ***DHCP*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***DHCP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN

	side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

PPPoE



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type:	PPPoE
User Name:	
Password:	
Service Name:	
Connection Type:	Continuous [Connect] [Disconnect]
Idle Time:	5 (1-1000 minutes)
MTU Size:	1452 (1360-1492 bytes)

○ Attain DNS Automatically

● Set DNS Manually

DNS 1:	8.8.8.8
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

□ Enable FTP Server Access on WAN

☑ Enable IPsec pass through on VPN connection

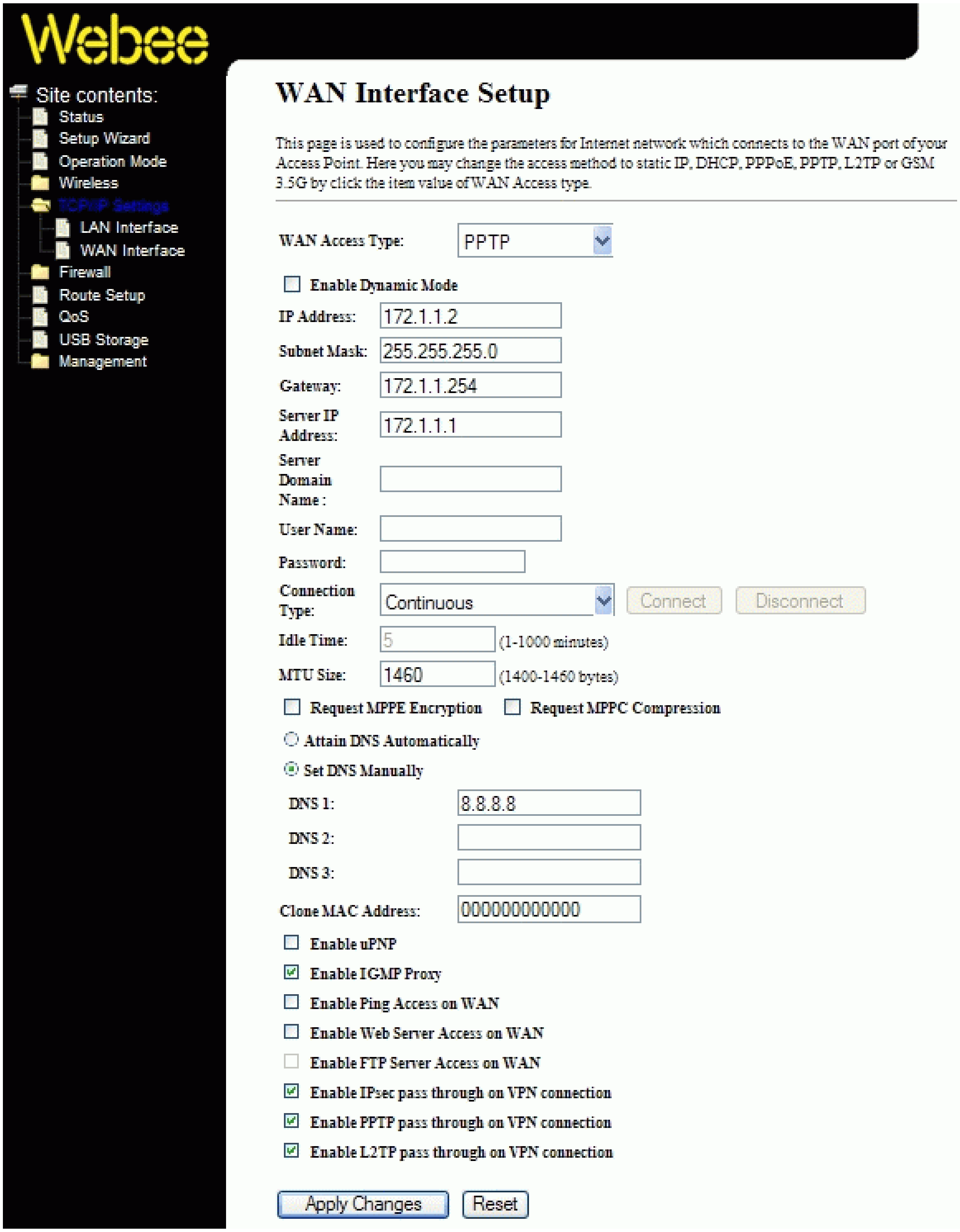
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

Item	Description
PPPoE	Click to select PPPoE support on WAN interface. There are user name, password, connection type and idle time settings need to be done.
User Name	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Password	If you select the PPPoE support on WAN interface, fill in the user name and password to login the PPPoE server.
Service Name	Fill in the service name of Service Name. The default value is empty.
Connection Type	Select the connection type from pull-down menu. There are ***Continuous***, ***Connect on Demand*** and ***Manual*** three types to select.

	Continuous connection type means to setup the connection through PPPoE protocol whenever this WLAN Broadband Router is powered on. ***Connect on Demand*** connection type means to setup the connection through PPPoE protocol whenever you send the data packets out through the WAN interface; there are a watchdog implemented to close the PPPoE connection while there are no data sent out longer than the idle time set. ***Manual*** connection type means to setup the connection through the PPPoE protocol by clicking the ***Connect*** button manually, and clicking the ***Disconnect*** button manually.
Idle Time	If you select the ***PPPoE*** and ***Connect on Demand*** connection type, fill in the idle time for auto-disconnect function. Value can be between 1 and 1000 minutes.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1452. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Attain DNS Automatically	Click to select getting DNS address for ***PPPoE*** support. Please select ***Set DNS Manually*** if the ***PPPoE*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***Static IP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

PPTP



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type: PPTP

☐ Enable Dynamic Mode

IP Address: 172.1.1.2

Subnet Mask: 255.255.255.0

Gateway: 172.1.1.254

Server IP Address: 172.1.1.1

Server Domain Name :

User Name:

Password:

Connection Type: Continuous

Idle Time: 5 (1-1000 minutes)

MTU Size: 1460 (1400-1460 bytes)

☐ Request MPPE Encryption ☐ Request MPPC Compression

○ Attain DNS Automatically

● Set DNS Manually

DNS 1: 8.8.8.8

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

☐ Enable uPNP

☑ Enable IGMP Proxy

☐ Enable Ping Access on WAN

☐ Enable Web Server Access on WAN

☐ Enable FTP Server Access on WAN

☑ Enable IPsec pass through on VPN connection

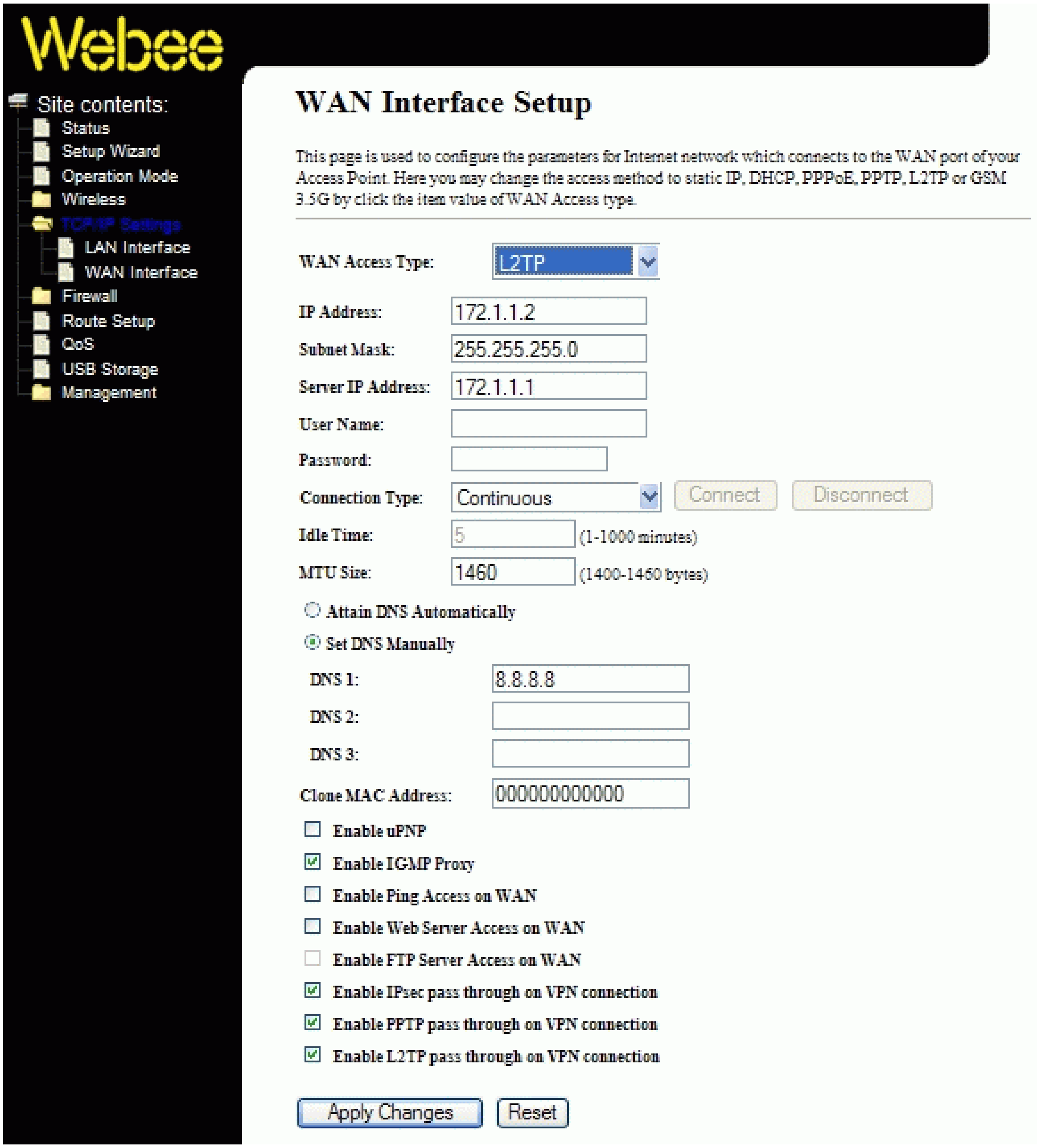
☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

Item	Description

PPTP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection.
Enable Dynamic Mode	Click to select PPTP Dynamic support on WAN interface for IP address assigned automatically from a PPTP server.
IP Address	If you select the PPTP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the PPTP support on WAN interface, fill in the subnet mask for it.
Gateway	If you select the Static PPTP support on WAN interface, fill in the gateway for WAN interface out going data packets.
Server IP Address	Enter the IP address of the PPTP Server.
Server Domain Name	Assign Domain Name and dispatch to PPTP servers. It is optional field.
User Name	If you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
Password	f you select the PPTP support on WAN interface, fill in the user name and password to login the PPTP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Request MPPE Encryption	Click the checkbox to enable request MPPE encryption.
Attain DNS Automatically	Click to select getting DNS address for ***PPTP*** support. Please select ***Set DNS Manually*** if the ***PPTP*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***PPTP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

L2TP



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type:	L2TP
IP Address:	172.1.1.2
Subnet Mask:	255.255.255.0
Server IP Address:	172.1.1.1
User Name:	
Password:	
Connection Type:	Continuous
Idle Time:	5 (1-1000 minutes)
MTU Size:	1460 (1400-1460 bytes)

○ Attain DNS Automatically

● Set DNS Manually

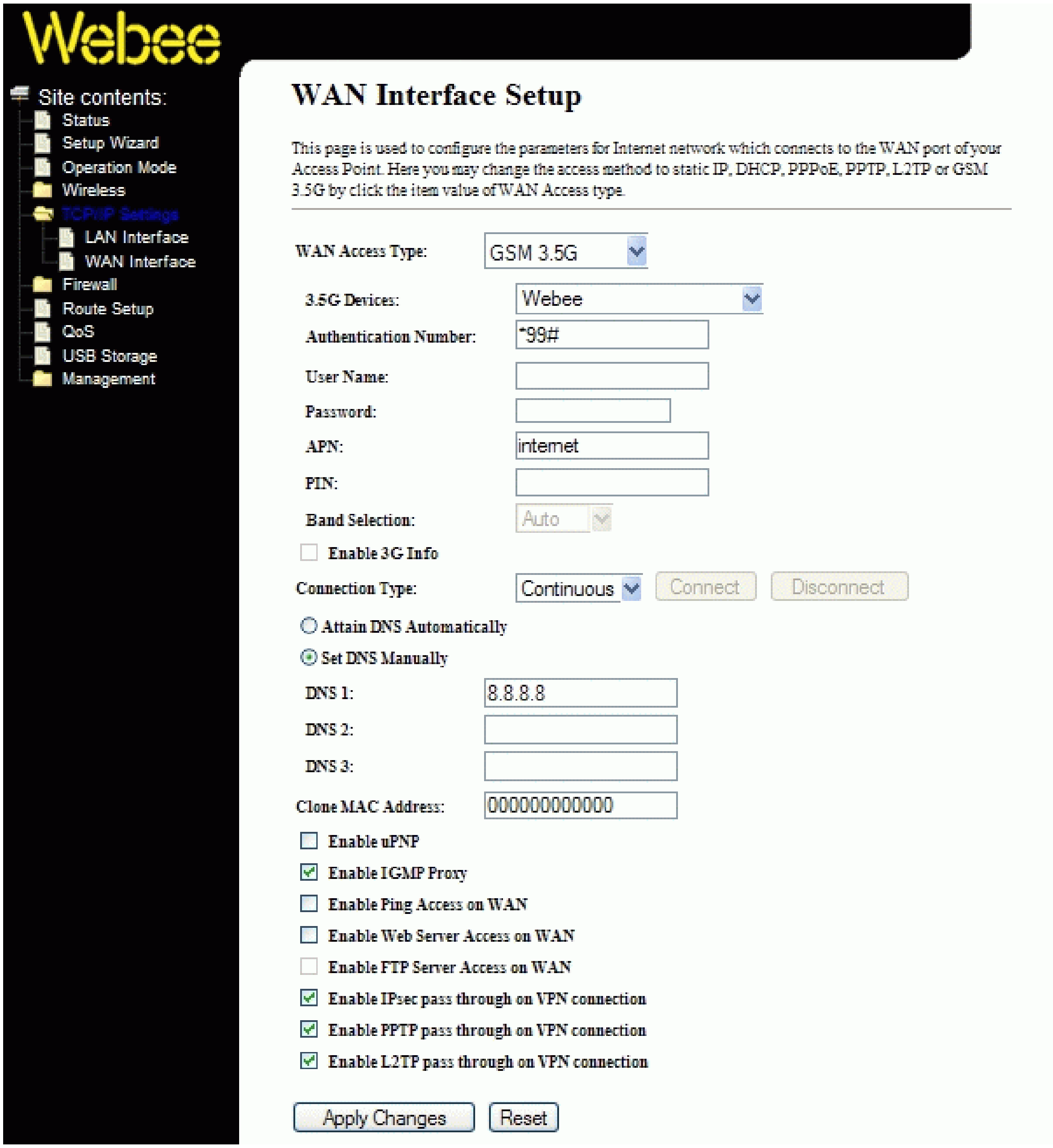
DNS 1:	8.8.8.8
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

□ Enable uPNP
☑ Enable IGMP Proxy
□ Enable Ping Access on WAN
□ Enable Web Server Access on WAN
□ Enable FTP Server Access on WAN
☑ Enable IPsec pass through on VPN connection
☑ Enable PPTP pass through on VPN connection
☑ Enable L2TP pass through on VPN connection

Item	Description
L2TP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection.
IP Address	If you select the L2TP support on WAN interface, fill in the IP address for it.
Subnet Mask	If you select the L2TP support on WAN interface, fill in the

	subnet mask for it.
Gateway	If you select the Static L2TP support on WAN interface, fill in the gateway for WAN interface out going data packets.
Server IP Address	Enter the IP address of the L2TP Server.
User Name	If you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
Password	f you select the L2TP support on WAN interface, fill in the user name and password to login the L2TP server.
MTU Size	Fill in the mtu size of MTU Size. The default value is 1460. Refer to 4.23 What is Maximum Transmission Unit (MTU) Size?
Attain DNS Automatically	Click to select getting DNS address for ***L2TP*** support. Please select ***Set DNS Manually*** if the ***L2TP*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***L2TP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

GSM3.5G



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type: GSM 3.5G

3.5G Devices: Webee

Authentication Number: *99#

User Name:

Password:

APN: internet

PIN:

Band Selection: Auto

□ Enable 3G Info

Connection Type: Continuous [Connect] [Disconnect]

○ Attain DNS Automatically

● Set DNS Manually

DNS 1: 8.8.8.8

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

□ Enable FTP Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

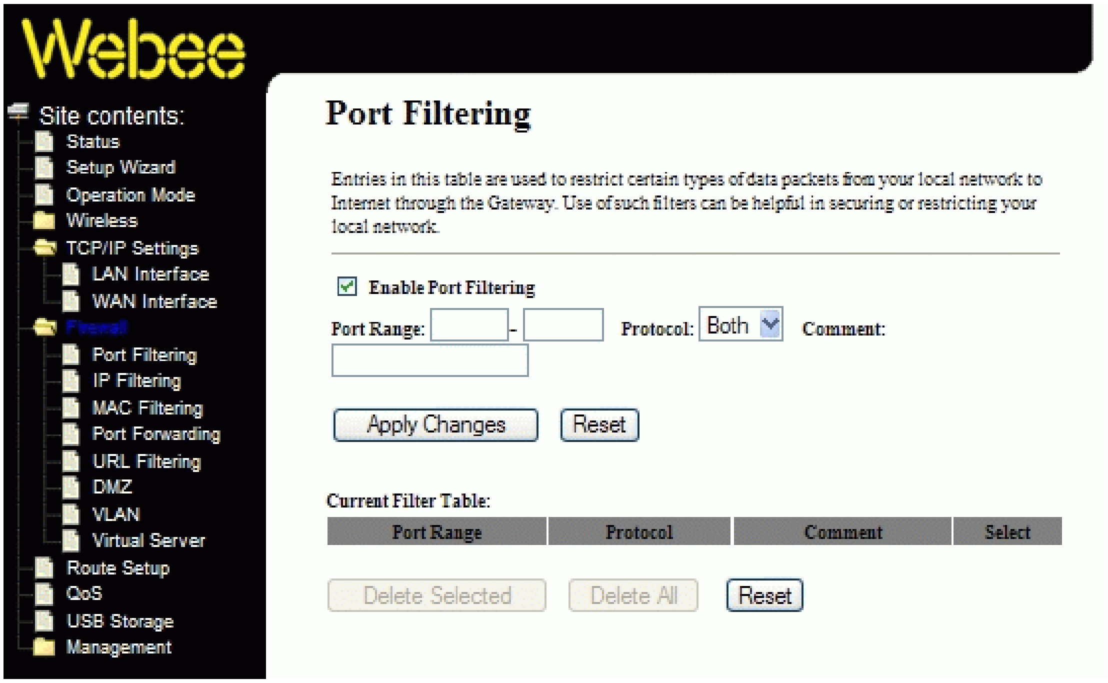
[Apply Changes] [Reset]

Item	Description
GSM 3.5G	Click to select GSM 3.5G support on WAN interface. There are 3.5G Devices, Authentication Number and APN settings need to be done.
3.5G Devices	Select 3.5G device, this version supports HuaWei E220, E180, E172 and E270.

Authentication Number	Please fill in Authentication Number from operator.
User Name	Please fill in user name from operator.
Password	Please fill in password from operator.
APN	Please fill in APN(Access Point Name) from operator.
Attain DNS Automatically	Click to select getting DNS address for ***GSM 3.5G*** support. Please select ***Set DNS Manually*** if the ***GSM 3.5G*** support is selected.
Set DNS Manually	Click to select getting DNS address for ***Static IP*** support.
DNS 1	Fill in the IP address of Domain Name Server 1.
DNS 2	Fill in the IP address of Domain Name Server 2.
DNS 3	Fill in the IP address of Domain Name Server 3.
Clone MAC Address	Fill in the MAC address that is the MAC address to be cloned. Refer to 4.24 What is Clone MAC Address?
Enable uPNP	Click the checkbox to enable uPNP function. Refer to 4.22 What is Universal Plug and Play (uPNP)?
Enable IGMP Proxy	Click the checkbox to enable IGMP Proxy.
Enable Ping Access on WAN	Click the checkbox to enable WAN ICMP response.
Enable Web Server Access on WAN	Click the checkbox to enable web configuration from WAN side.
Enable FTP Server Access on WAN	Click the checkbox to enable FTP Server Access on WAN
Enable IPsec pass through on VPN connection	Click the checkbox to enable IPSec packet pass through
Enable PPTP pass through on VPN connection	Click the checkbox to enable PPTP packet pass through
Enable L2TP pass through on VPN connection	Click the checkbox to enable L2TP packet pass through
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.15 Firewall - Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable Port Filtering

Port Range: ______ - ______ Protocol: Both Comment: ______

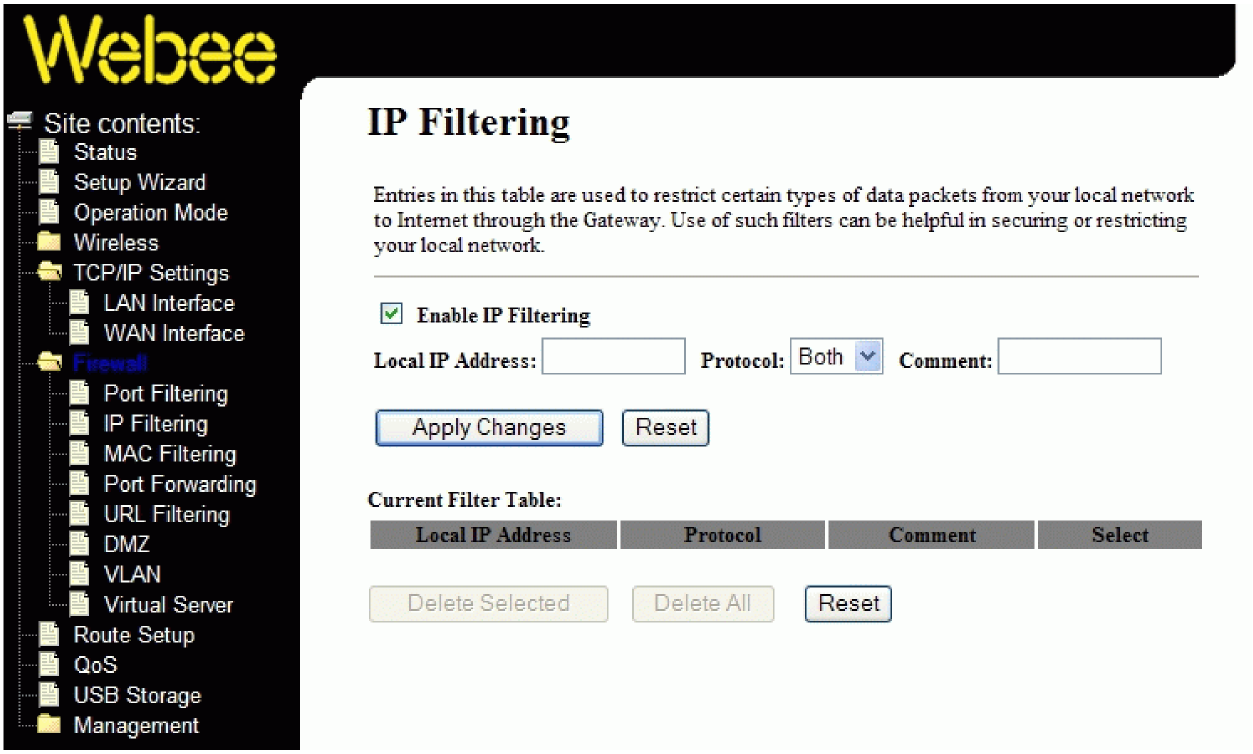
Current Filter Table:

Port Range	Protocol	Comment	Select

Item	Description
Enable Port Filtering	Click to enable the port filtering security function.
Port Range Protocol Comments	To restrict data transmission from the local network on certain ports, fill in the range of start-port and end-port, and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the ports.
Apply Changes	Click the ***Apply Changes*** button to register the ports to port filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected port range that will be removed from the port-filtering list.
Delete All	Click to delete all the registered entries from the port-filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.16 Firewall - IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable IP Filtering

Local IP Address: Protocol: Both Comment:

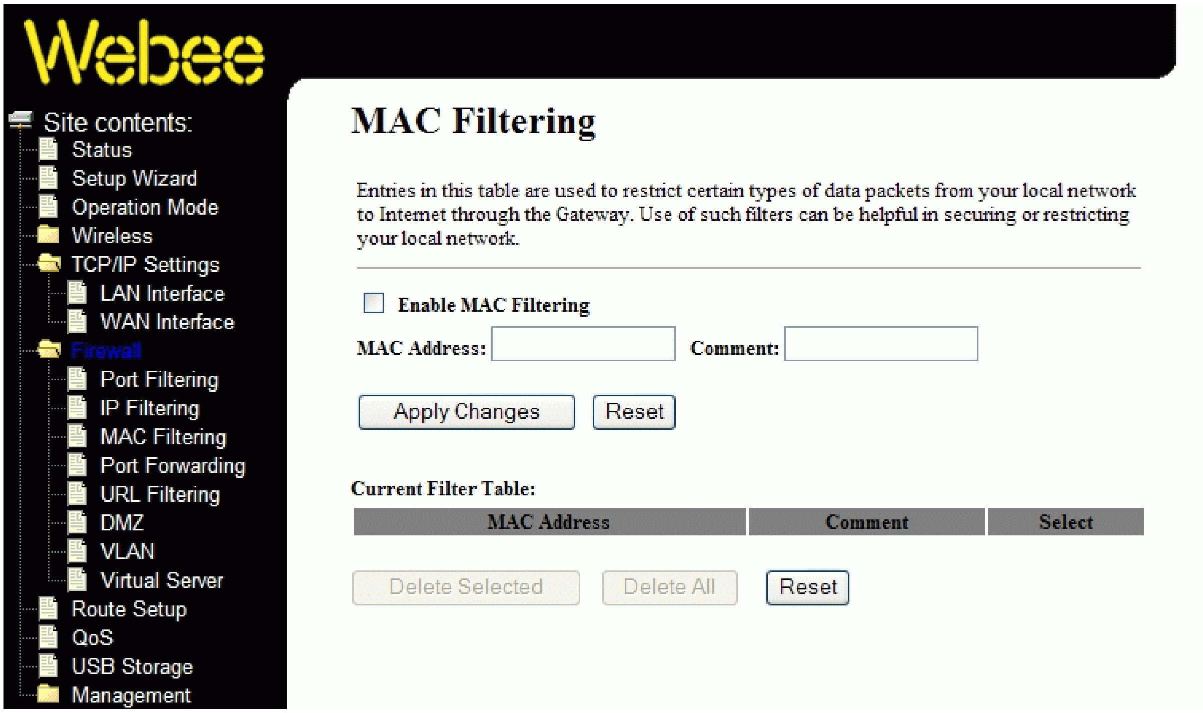
Current Filter Table:

Local IP Address	Protocol	Comment	Select

Item	Description
Enable IP Filtering	Click to enable the IP filtering security function.
Local IP Address Protocol Comments	To restrict data transmission from local network on certain IP addresses, fill in the IP address and the protocol, also put your comments on it. The ***Protocol*** can be TCP, UDP or Both. ***Comments*** let you know about whys to restrict data from the IP address.
Apply Changes	Click the ***Apply Changes*** button to register the IP address to IP filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address that will be removed from the IP-filtering list.
Delete All	Click to delete all the registered entries from the IP-filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.17 Firewall - MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable MAC Filtering

MAC Address: ______ Comment: ______

Apply Changes | Reset

Current Filter Table:

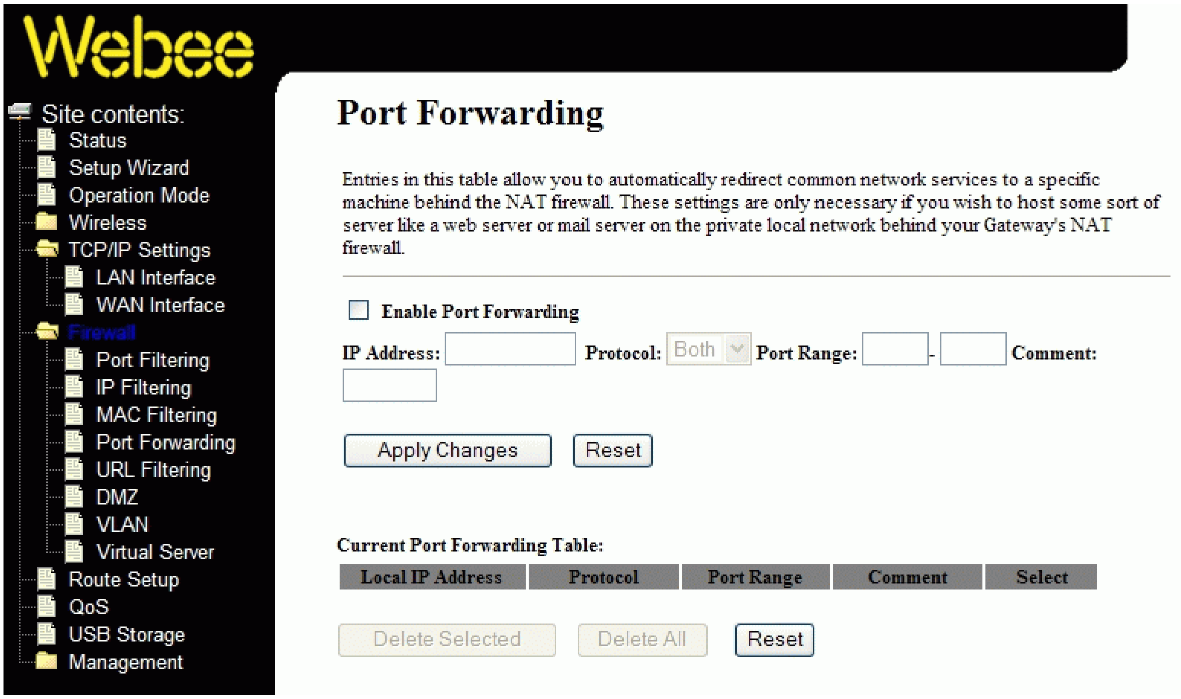
MAC Address	Comment	Select

Delete Selected | Delete All | Reset

Item	Description
Enable MAC Filtering	Click to enable the MAC filtering security function.
MAC Address Comments	To restrict data transmission from local network on certain MAC addresses, fill in the MAC address and your comments on it. ***Comments*** let you know about whys to restrict data from the MAC address.
Apply Changes	Click the ***Apply Changes*** button to register the MAC address to MAC filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected MAC address that will be removed from the MAC-filtering list.
Delete All	Click to delete all the registered entries from the MAC-filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.18 Firewall - Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

□ Enable Port Forwarding

IP Address: ____ Protocol: Both Port Range: ____ - ____ Comment: ____

Apply Changes | Reset

Current Port Forwarding Table:

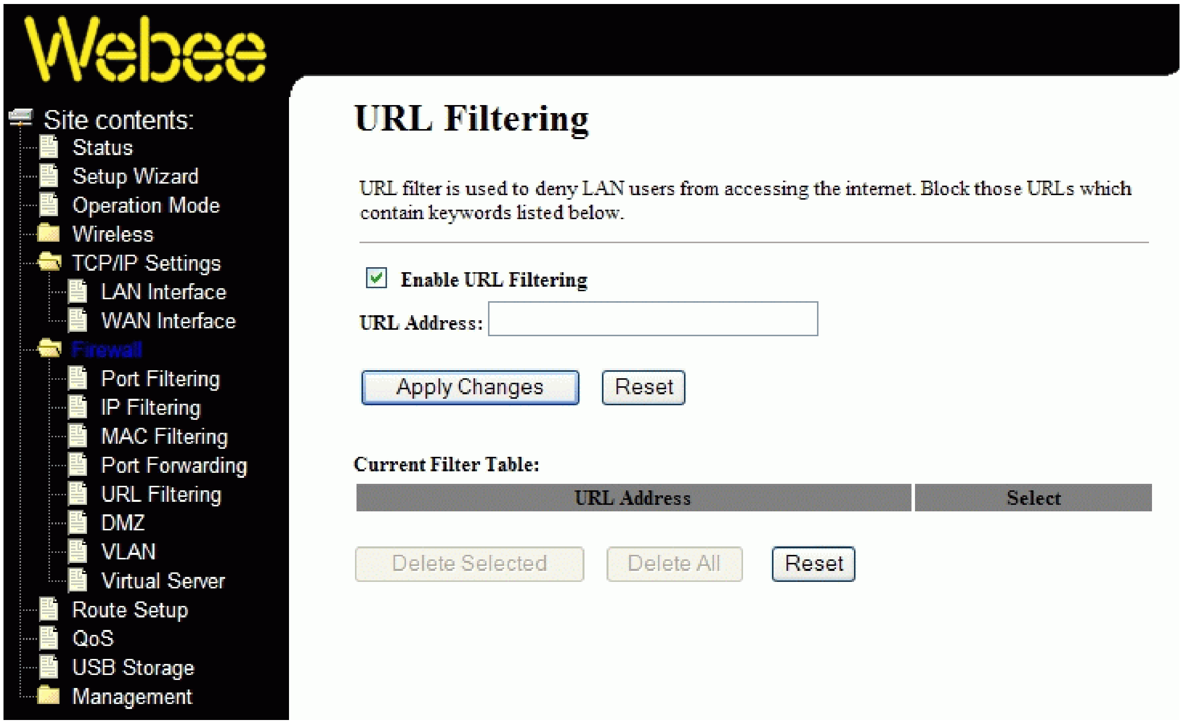
Local IP Address	Protocol	Port Range	Comment	Select

Delete Selected | Delete All | Reset

Item	Description
Enable Port Forwarding	Click to enable the Port Forwarding security function.
IP Address Protocol Port Range Comment	To forward data packets coming from WAN to a specific IP address that hosted in local network behind the NAT firewall, fill in the IP address, protocol, port range and your comments. The ***Protocol*** can be TCP, UDP or Both. The ***Port Range*** for data transmission. ***Comments*** let you know about whys to allow data packets forward to the IP address and port number.
Apply Changes	Click the ***Apply Changes*** button to register the IP address and port number to Port forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.19 Firewall – URL Filtering

URL Filtering is used to restrict users to access specific websites in internet.



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☑ Enable URL Filtering

URL Address:

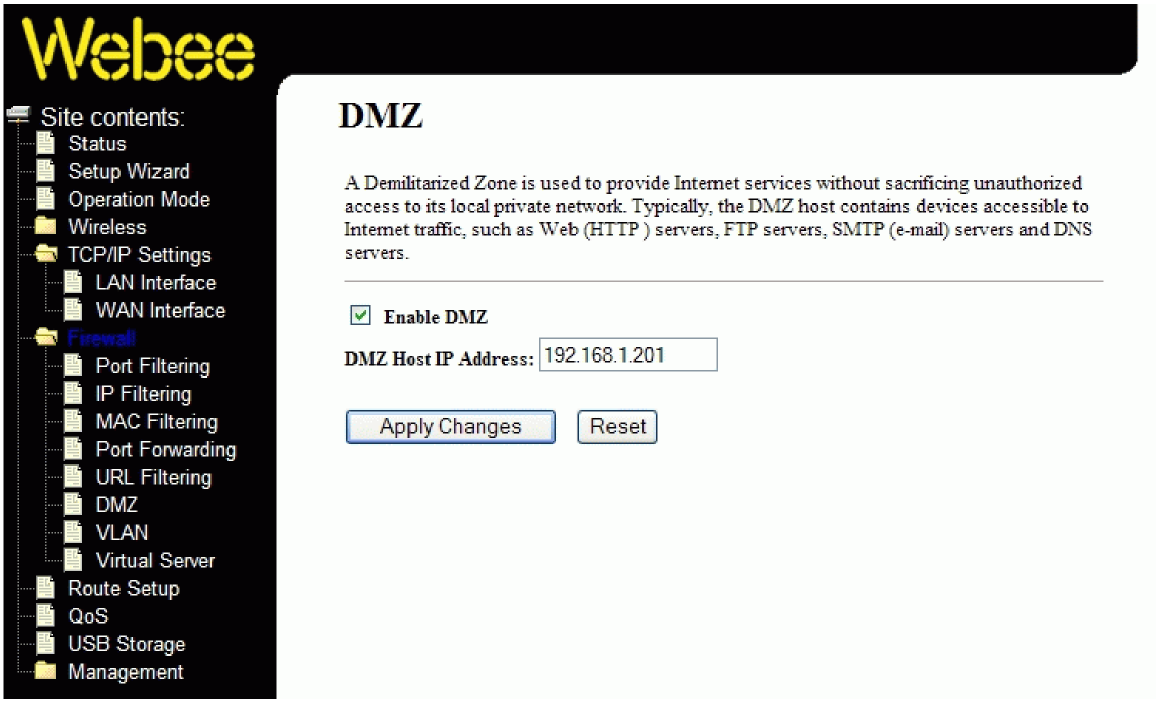
Current Filter Table:

URL Address	Select

Item	Description
Enable URL Filtering	Click to enable the URL Filtering function.
URL Address	Add one URL address.
Apply Changes	Click the ***Apply Changes*** button to save settings.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected URL address that will be removed from the URL Filtering list.
Delete All	Click to delete all the registered entries from the URL Filtering list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.20 Firewall – DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

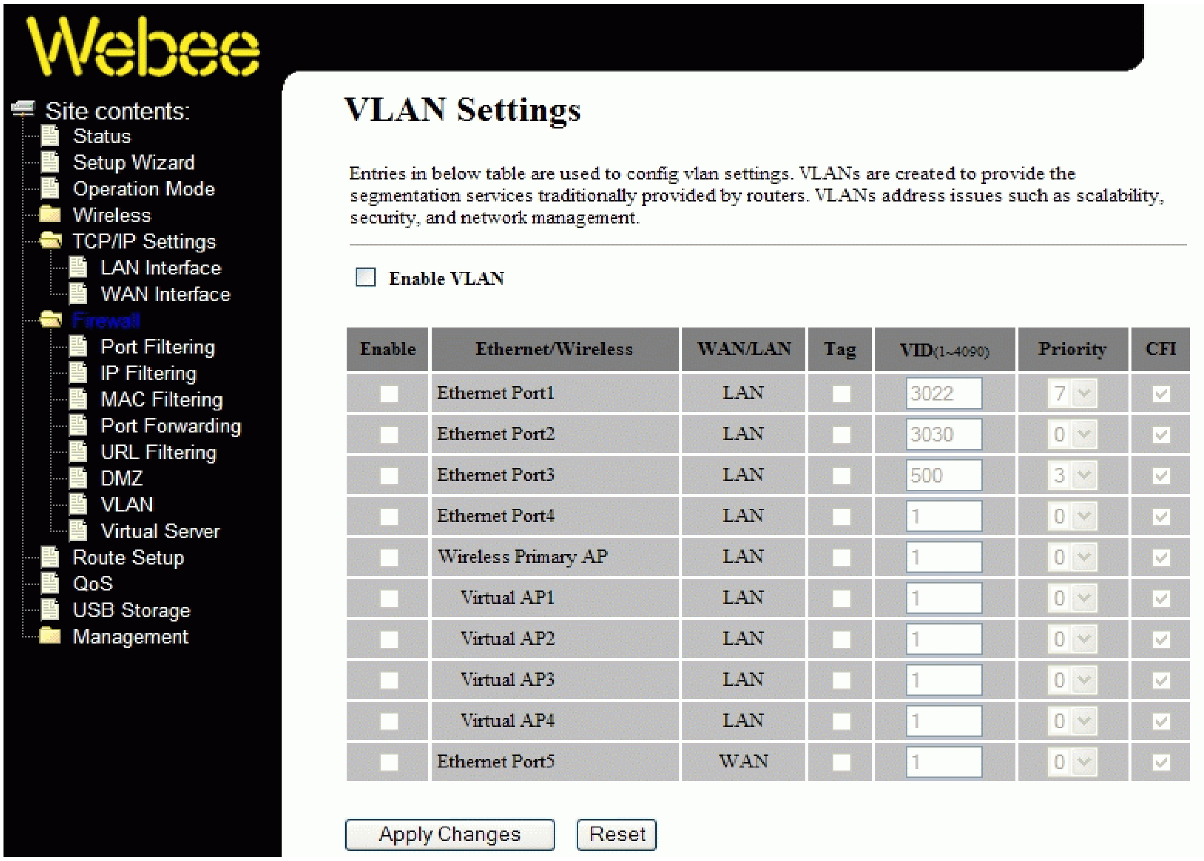
☑ Enable DMZ

DMZ Host IP Address: 192.168.1.201

Item	Description
Enable DMZ	Click to enable the DMZ function.
DMZ Host IP Address	To support DMZ in your firewall design, fill in the IP address of DMZ host that can be access from the WAN interface.
Apply Changes	Click the ***Apply Changes*** button to register the IP address of DMZ host.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.21 Firewall – VLAN

Entries in this table could configure wired or wireless VLAN settings for scalability, security and network management.



VLAN Settings

Entries in below table are used to config vlan settings. VLANs are created to provide the segmentation services traditionally provided by routers. VLANs address issues such as scalability, security, and network management.

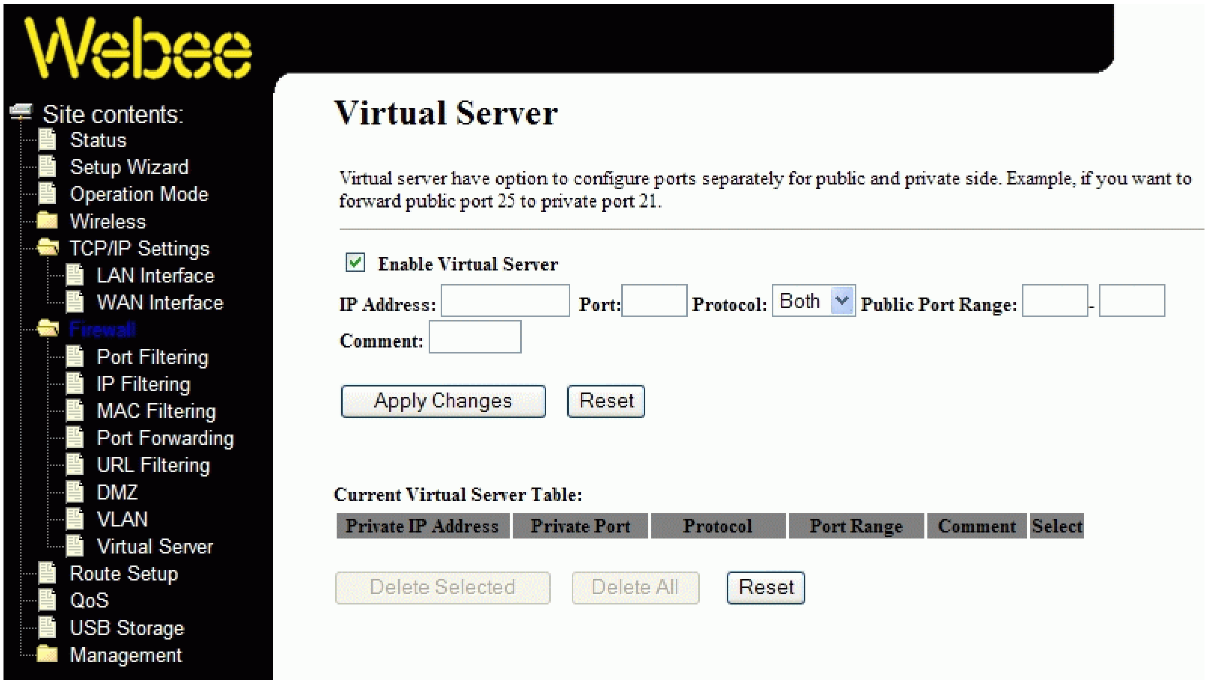
□ **Enable VLAN**

Enable	Ethernet/Wireless	WAN/LAN	Tag	VID(1~4090)	Priority	CFI
□	Ethernet Port1	LAN	□	3022	7	☑
□	Ethernet Port2	LAN	□	3030	0	☑
□	Ethernet Port3	LAN	□	500	3	☑
□	Ethernet Port4	LAN	□	1	0	☑
□	Wireless Primary AP	LAN	□	1	0	☑
□	Virtual AP1	LAN	□	1	0	☑
□	Virtual AP2	LAN	□	1	0	☑
□	Virtual AP3	LAN	□	1	0	☑
□	Virtual AP4	LAN	□	1	0	☑
□	Ethernet Port5	WAN	□	1	0	☑

Item	Description
Enable VLAN	Click to enable the LAN function.
Enable	Click Enable Ethernet LAN port, Wireless, AP or WAN port.
Tag	When 'Tag' is enabled, Router will add a 802.1Q tagging (4 bytes long w/ VID, Priority, and CFI) in the header of each outgoing packet.
VID	The VID on WAN and LAN port need not be the same. When the packet is forwarded from LAN to WAN, the VID of LAN port will be carried to WAN port. Also, when packet is come from WAN to LAN, router will forward this packet to the LAN port, with matched VID.
Priority	Select port priority.
CFI	Click to Enable CFI.

4.3.22 Firewall – Virtual Server

Entries in this table allow you to redirect specific public port to private ports in local network behind your Gateway's NAT firewall.



Virtual Server

Virtual server have option to configure ports separately for public and private side. Example, if you want to forward public port 25 to private port 21.

☑ Enable Virtual Server

IP Address: Port: Protocol: Both Public Port Range: -

Comment:

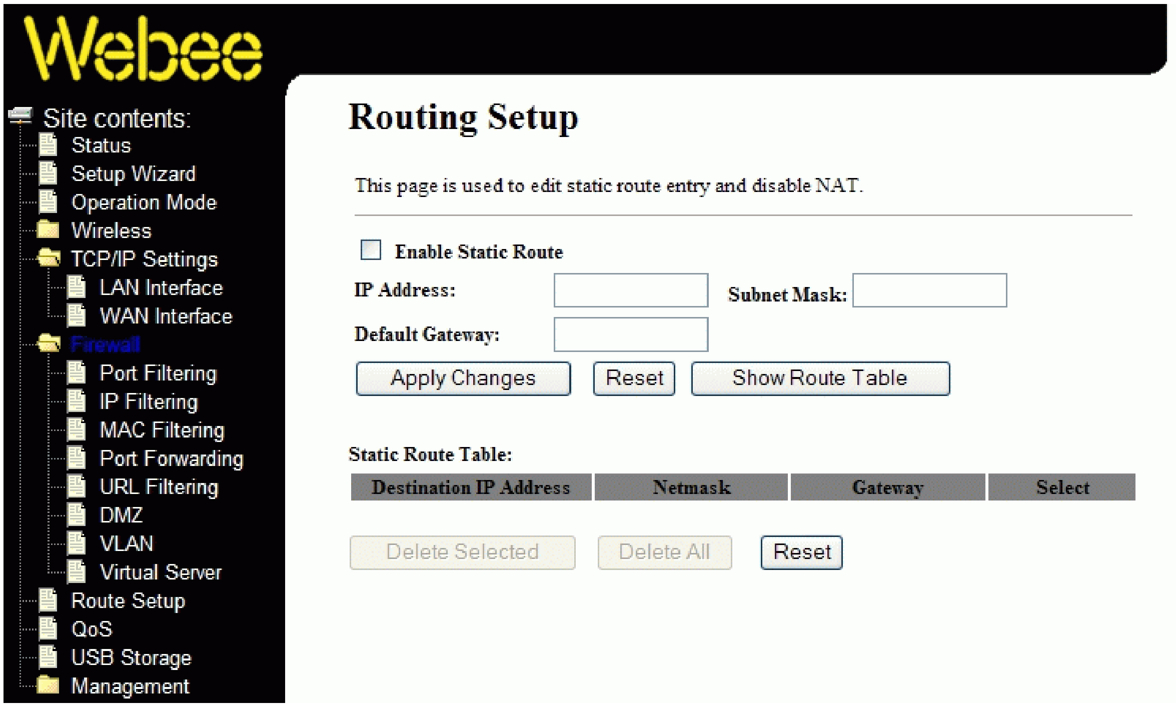
Current Virtual Server Table:

Private IP Address	Private Port	Protocol	Port Range	Comment	Select

Item	Description
Enable Virtual Server	Click to enable the Virtual Server function.
IP Address	The ***IP Address*** for local ip address.
Port	The ***Port*** for local private port
Protocol	The ***Protocol*** can be TCP, UDP or Both.
Public Port Range	The ***Public Port Range*** for public service ports range.
Comment	***Comments*** let you know about whys to allow data packets forward to the IP address and port number.
Apply Changes	Click the ***Apply Changes*** button to register the IP address and port number to Port forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Delete Selected	Click to delete the selected IP address and port number that will be removed from the port-forwarding list.
Delete All	Click to delete all the registered entries from the port-forwarding list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.23 Route Setup

This page is used to edit static route entry and disable NAT.



Routing Setup

This page is used to edit static route entry and disable NAT.

☐ Enable Static Route

IP Address: Subnet Mask:

Default Gateway:

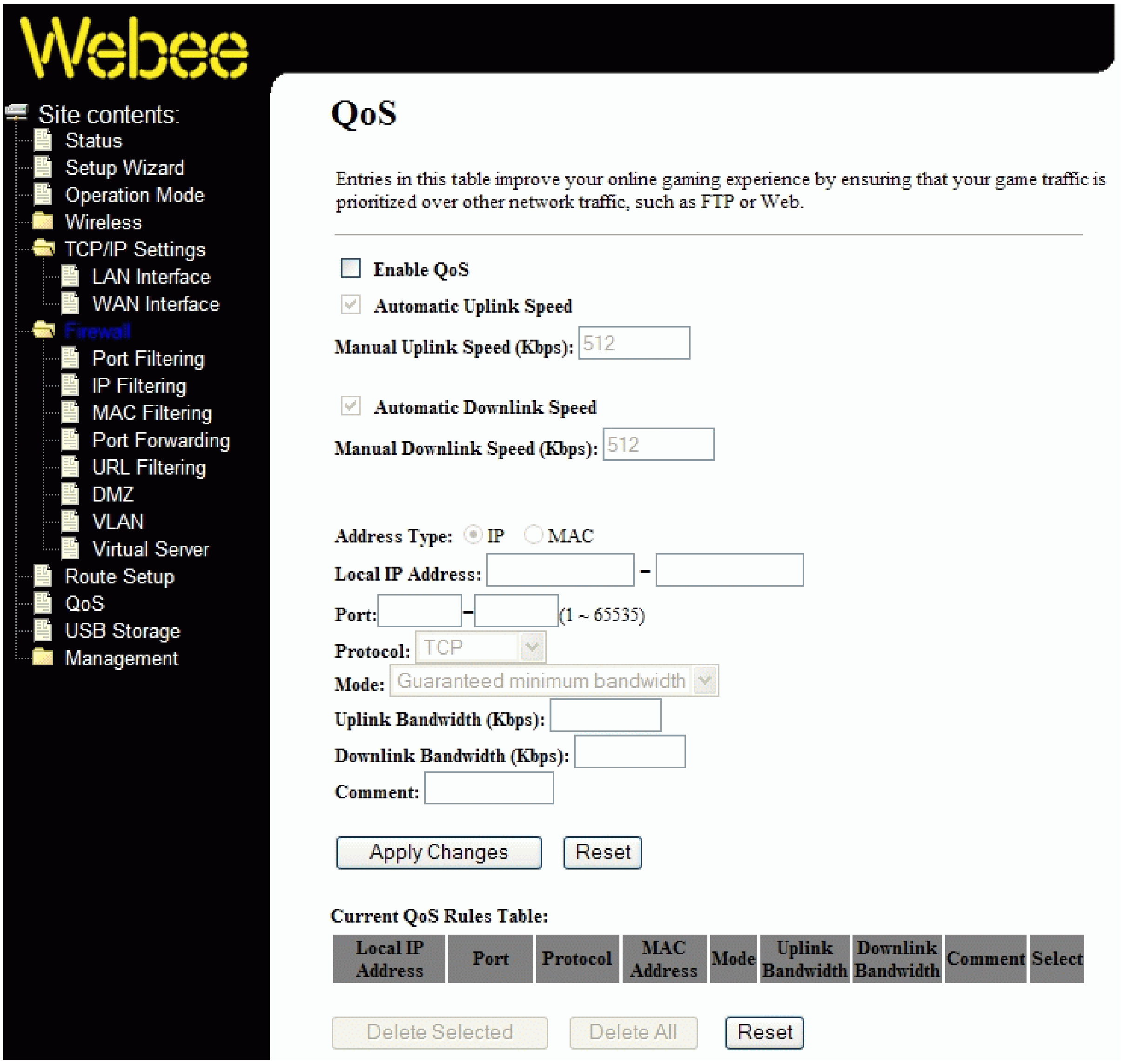
Static Route Table:

Destination IP Address	Netmask	Gateway	Select

Item	Description
Enable Static Route	Click to Enable the Static Route function
IP Address Subnet Mask Default Gateway	Manually Specify the packets arrive at the destination. The internal network can be avoided through the Internet of the packet exchange.
Apply Changes	Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Show Route Table	Click button to show route table
Delete All	Click to delete all the registered entries from static route table list..
Delete Select	Click to delete the selected rout table that will be removed from the static route table list.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.24 QoS

This page provides multi remote and local end points quality of service.



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

□ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 512

Address Type: ● IP ○ MAC

Local IP Address: ____ - ____

Port: ____ - ____ (1 ~ 65535)

Protocol: TCP

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps): ____

Downlink Bandwidth (Kbps): ____

Comment: ____

Current QoS Rules Table:

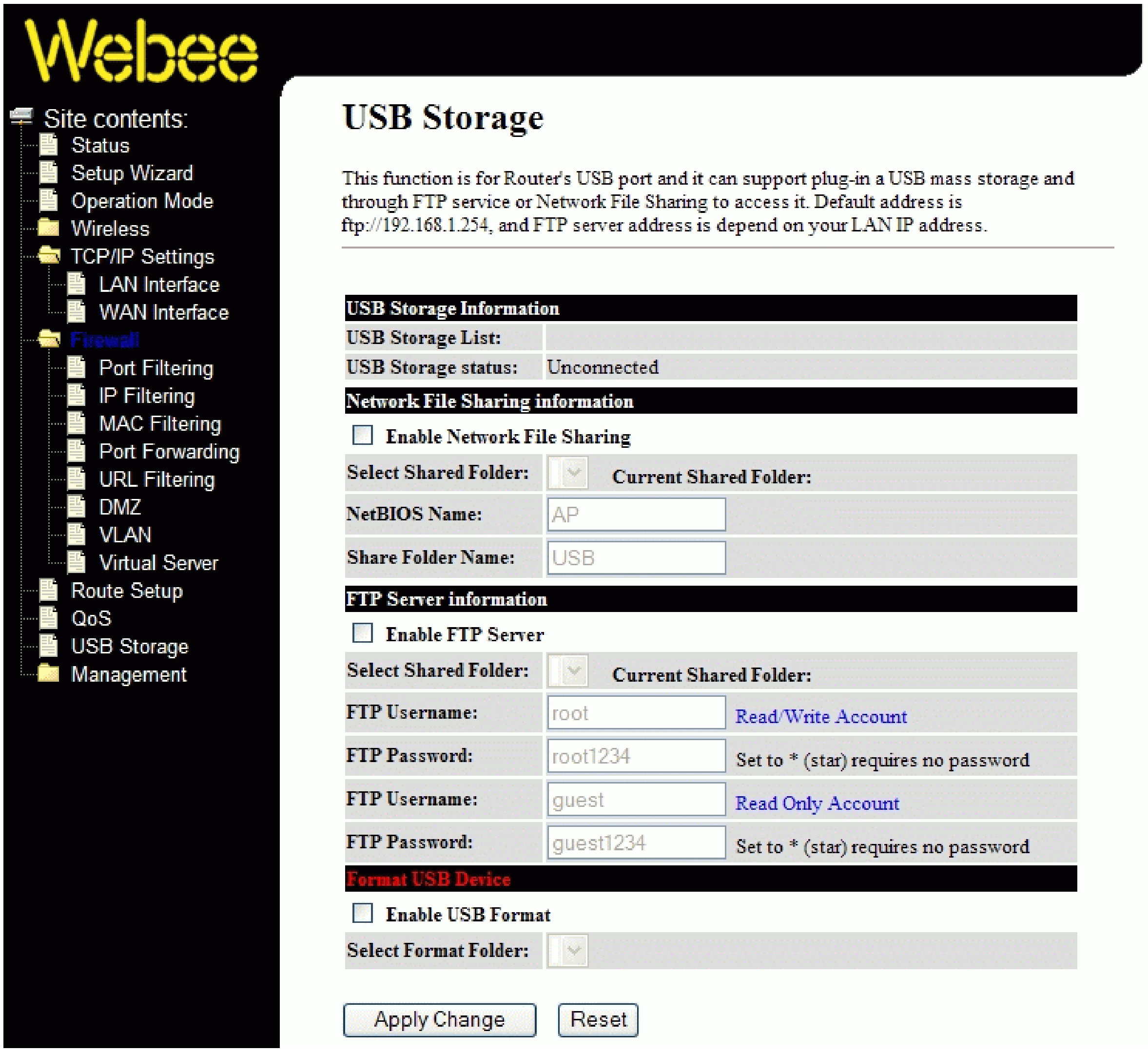
Local IP Address	Port	Protocol	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

Item	Description
Enable QoS	Click to enable the QoS function.
Automatic Uplink Speed	Click checkbox to enable Uplink speed by system.
Manual Uplink Speed(Kbps)	Input number to set Uplink speed.
Manual Downlink Speed(Kbps)	Click checkbox to enable Downlink speed by system.
Manual Downlink Speed(Kbps)	Input number to set Downlink speed.
Address Type	Click the set type either IP or MAC address.
Local IP	Input the range IP address of LAN.

Port	Input MAC address.
Protocol	The ***Protocol*** can be TCP, UDP, TCP/UDP, ICMP or ANY.
Mode	There are 2 options to control the bandwidth. One is ***Guaranteed minimum bandwidth***. The other is ***Restricted maximum bandwidth***.
Uplink bandwidth (Kbps)	Set Uplink bandwidth for range of IP addresses or specific MAC address
Downlink bandwidth (Kbps)	Set Downlink bandwidth for range of IP addresses or specific MAC address
Comment	Comment let you know about whys the restrict data from the QoS
Apply Change	Click ***Apply Change*** button to register the QoS list
Reset	Click ***Reset*** button to abort change and recover the previous configuration setting.

4.3.25 USB Storage

This page provides USB storage management like USB link status, network file sharing, ftp server and USB FAT32 format tool.



USB Storage

This function is for Router's USB port and it can support plug-in a USB mass storage and through FTP service or Network File Sharing to access it. Default address is ftp://192.168.1.254, and FTP server address is depend on your LAN IP address.

USB Storage Information

USB Storage List:	
USB Storage status:	Unconnected

Network File Sharing information

□ Enable Network File Sharing

Select Shared Folder:		Current Shared Folder:
NetBIOS Name:	AP	
Share Folder Name:	USB	

FTP Server information

□ Enable FTP Server

Select Shared Folder:		Current Shared Folder:
FTP Username:	root	Read/Write Account
FTP Password:	root1234	Set to * (star) requires no password
FTP Username:	guest	Read Only Account
FTP Password:	guest1234	Set to * (star) requires no password

Format USB Device

□ Enable USB Format

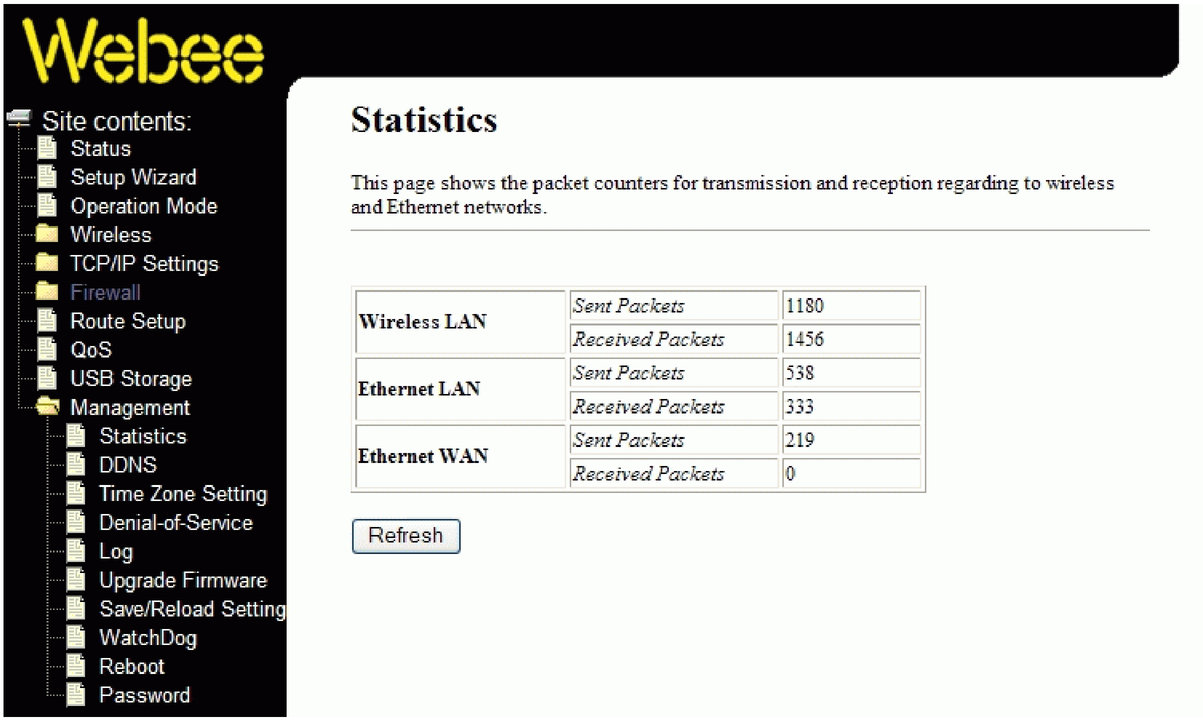
Select Format Folder:	

Item	Description
USB Storage Information	
USB Storage List	It lists mounted USB storage ID.
USB Storage Status	It shows USB storage link status.
Network File Sharing Information	
Enable Network File Sharing	Click to enable ***Network File Sharing***.
Select Share Folder	Click drop down menu to select which USB storage which you would like to share.
Current Share Folder	It shows the current share USB storage.
NetBIOS Name	Input **NetBIOS** name. Max character is 30.
Share Folder Name	Input ***Share Folder*** name. Max character is 30.
FTP Server Information	
Enable FTP Server	Click to enable ***FTP Server***.
Select Share Folder	Click drop down menu to select which USB storage which you would like to set as ***FTP Server***.
Current Share Folder	It shows the current FTP USB server.

FTP Username	Assign FTP server login name. Default is root. Read/Write Account.
FTP Password	Assign FTP server login password. Default is root1234.
FTP Username	Assign FTP server login name. Default is quest. Read only Account.
FTP Password	Assign FTP server login password. Default is quest1234.
Format USB Device	
Enable USB Format	Click to enable USB storage format tool.
Select Format Folder	Click drop down menu to select which USB storage you would like to format to FAT32.
Apply Change	Click the ***Apply Change*** button to save and enable services.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.26 Management – Statistics

This page shows the packet counters for transmission and reception regarding to wireless, Ethernet LAN and Ethernet WAN networks.



Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

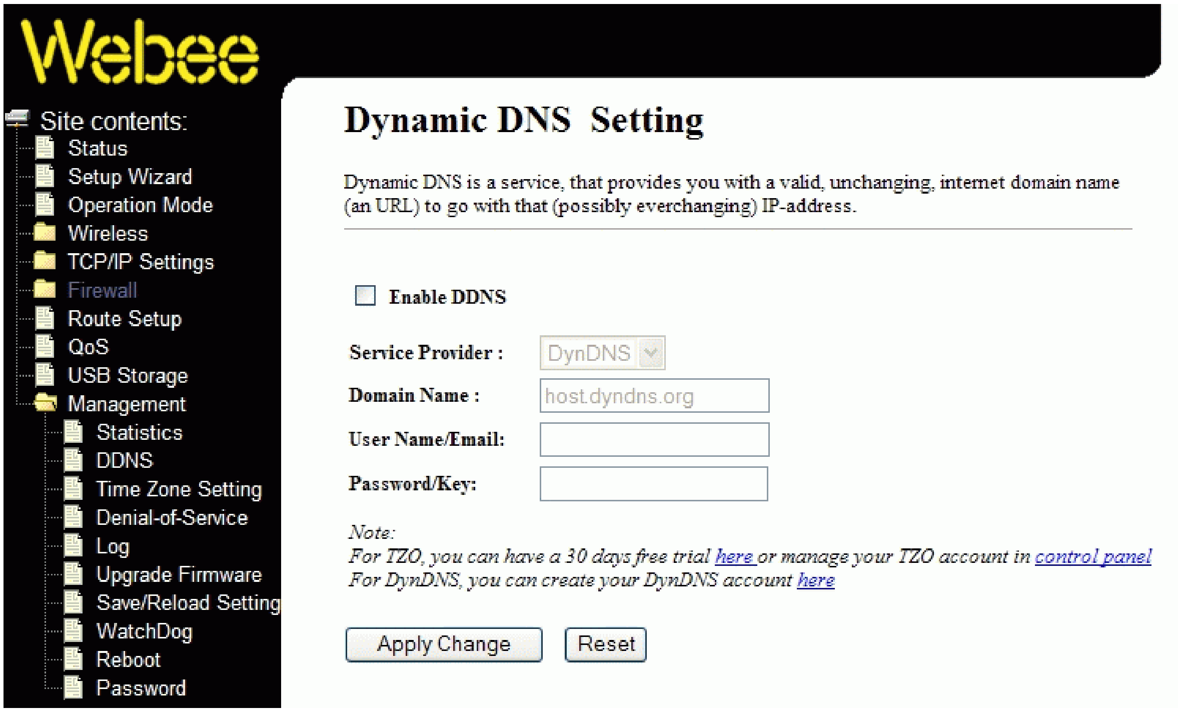
Wireless LAN	*Sent Packets*	1180
	Received Packets	1456
Ethernet LAN	*Sent Packets*	538
	Received Packets	333
Ethernet WAN	*Sent Packets*	219
	Received Packets	0

Item	Description
Wireless LAN ***Sent Packets***	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN ***Received Packets***	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN	It shows the statistic count of sent packets on the Ethernet LAN

Sent Packets	interface.
Ethernet LAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet LAN interface.
Ethernet WAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet WAN interface.
Ethernet WAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet WAN interface.
Refresh	Click the refresh the statistic counters on the screen.

4.3.27 Management – DDNS

This page is used to configure Dynamic DNS service to have DNS with dynamic IP address.



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☐ **Enable DDNS**

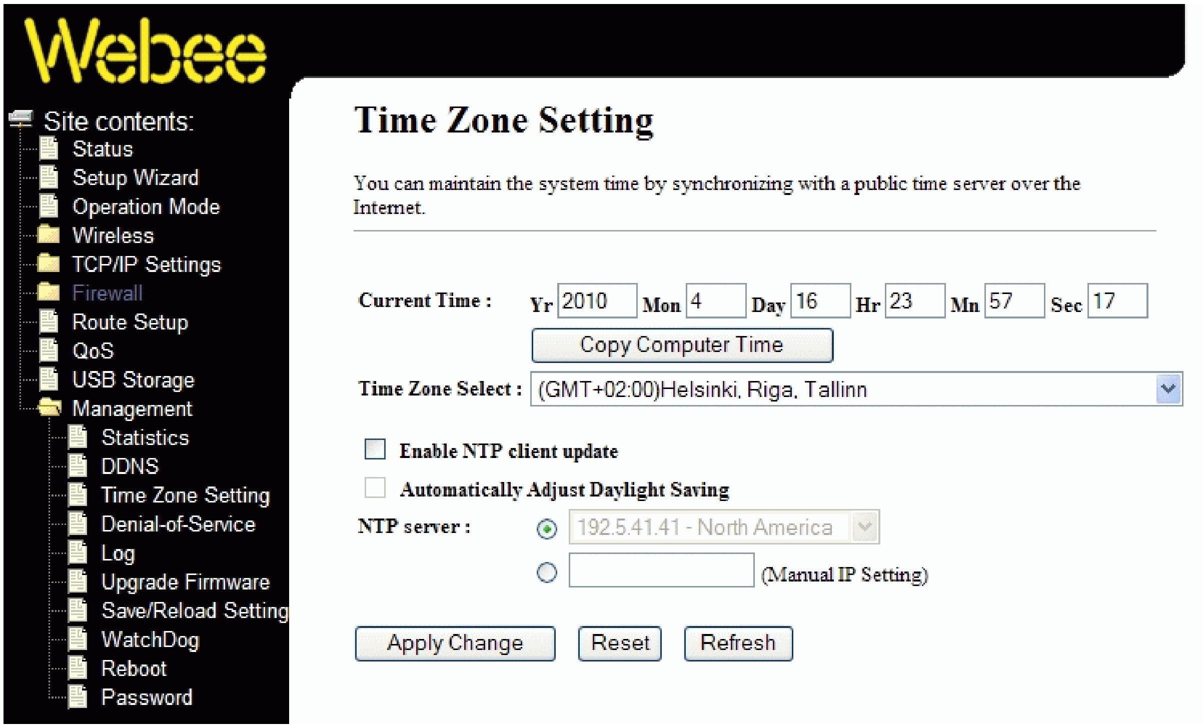
Service Provider :	DynDNS
Domain Name :	host.dyndns.org
User Name/Email:	
Password/Key:	

Note:
For TZO, you can have a 30 days free trial here or manage your TZO account in control panel
For DynDNS, you can create your DynDNS account here

Item	Description
Enable DDNS	Click the checkbox to enable ***DDNS*** service. Refer to 4.25 What is DDNS?
Service Provider	Click the drop down menu to pickup the right provider.
Domain Name	To configure the Domain Name.
User Name/Email	Configure User Name, Email.
Password/Key	Configure Password, Key.
Apply Change	Click the ***Apply Changes*** button to save and enable DDNS service.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.28 Management - Time Zone Setting

This page is used to configure NTP client to get current time.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2010 Mon 4 Day 16 Hr 23 Mn 57 Sec 17

Copy Computer Time

Time Zone Select : (GMT+02:00)Helsinki, Riga, Tallinn

□ Enable NTP client update

□ Automatically Adjust Daylight Saving

NTP server : ● 192.5.41.41 - North America

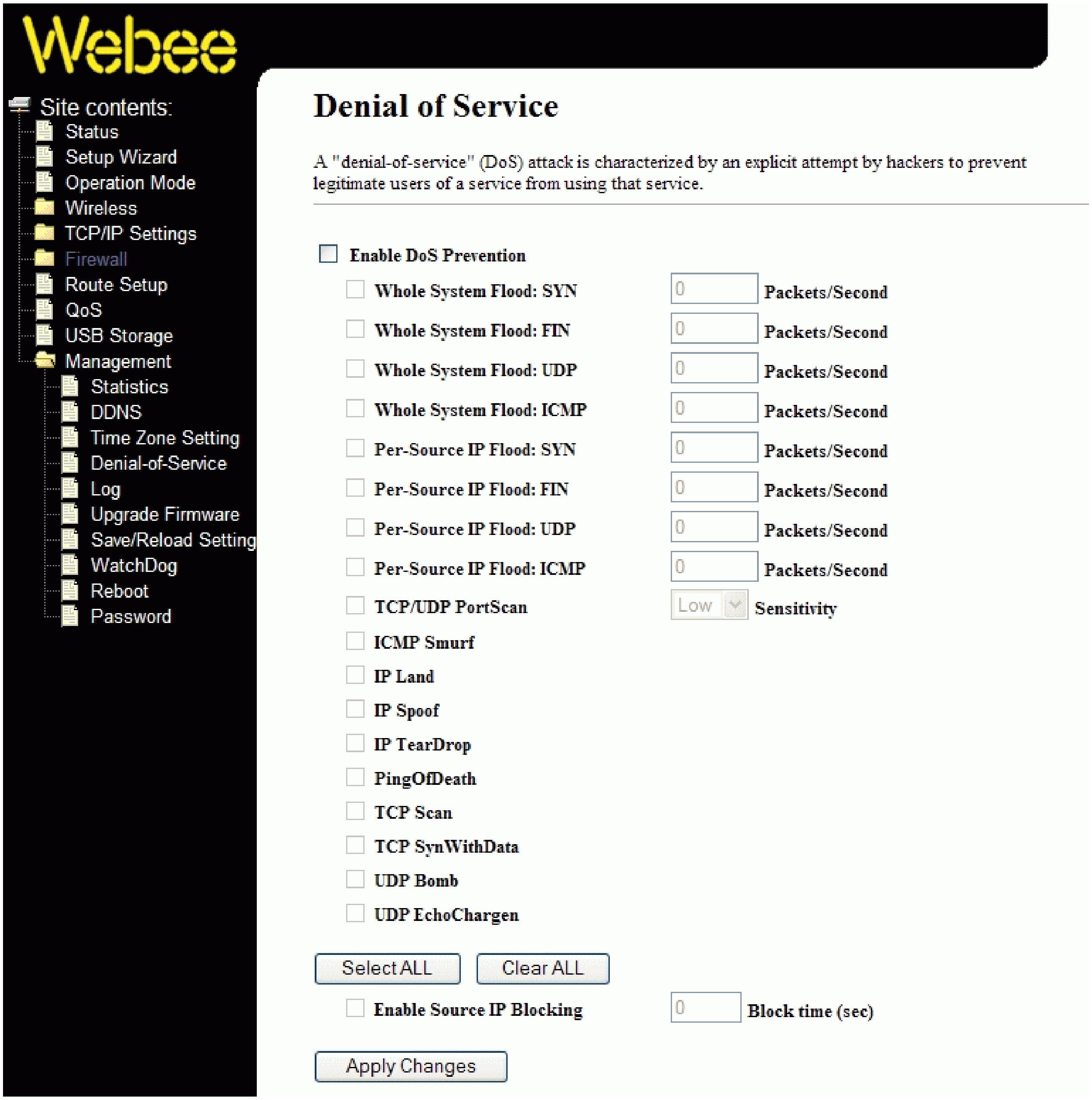
○ (Manual IP Setting)

Apply Change | Reset | Refresh

Item	Description
Current Time	It shows the current time.
Time Zone Select	Click the time zone in your country.
Enable NTP client update	Click the checkbox to enable NTP client update. Refer to 4.26 What is NTP Client?
Automatically Adjust Daylight Saving	Click to enable Daylight Saving adjustment automatically.
NTP Server	Click select default or input NTP server IP address.
Apply Change	Click the ***Apply Changes*** button to save and enable NTP client service.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.
Refresh	Click the refresh the current time shown on the screen.

4.3.29 Management – Denial-of-Service

This page is used to enable and setup protection to prevent attack by hacker’s program. It provides more security for users.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

□ Enable DoS Prevention

□ Whole System Flood: SYN 0 Packets/Second

□ Whole System Flood: FIN 0 Packets/Second

□ Whole System Flood: UDP 0 Packets/Second

□ Whole System Flood: ICMP 0 Packets/Second

□ Per-Source IP Flood: SYN 0 Packets/Second

□ Per-Source IP Flood: FIN 0 Packets/Second

□ Per-Source IP Flood: UDP 0 Packets/Second

□ Per-Source IP Flood: ICMP 0 Packets/Second

□ TCP/UDP PortScan Low Sensitivity

□ ICMP Smurf

□ IP Land

□ IP Spoof

□ IP TearDrop

□ PingOfDeath

□ TCP Scan

□ TCP SynWithData

□ UDP Bomb

□ UDP EchoChargen

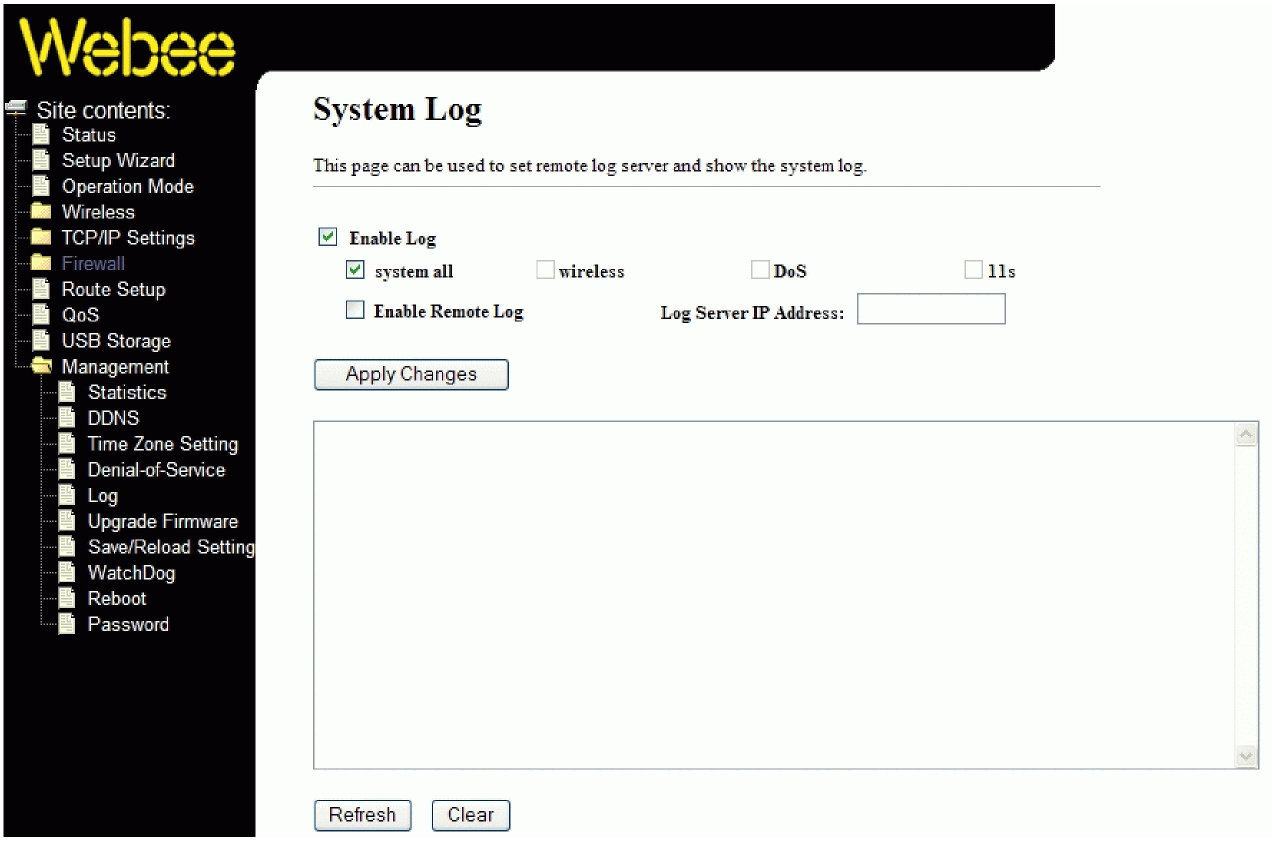
□ Enable Source IP Blocking 0 Block time (sec)

Item	Description
Enable DoS Prevention	Click the checkbox to enable DoS prevention.

Whole System Flood / Per-Source IP Flood…	Enable and setup prevention in details.
Select ALL	Click the checkbox to enable all prevention items.
Clear ALL	Click the checkbox to disable all prevention items.
Apply Changes	Click the ***Apply Changes*** button to save above settings.

4.3.30 Management – Log

This page is used to configure the remote log server and shown the current log.



System Log

This page can be used to set remote log server and show the system log.

☑ Enable Log

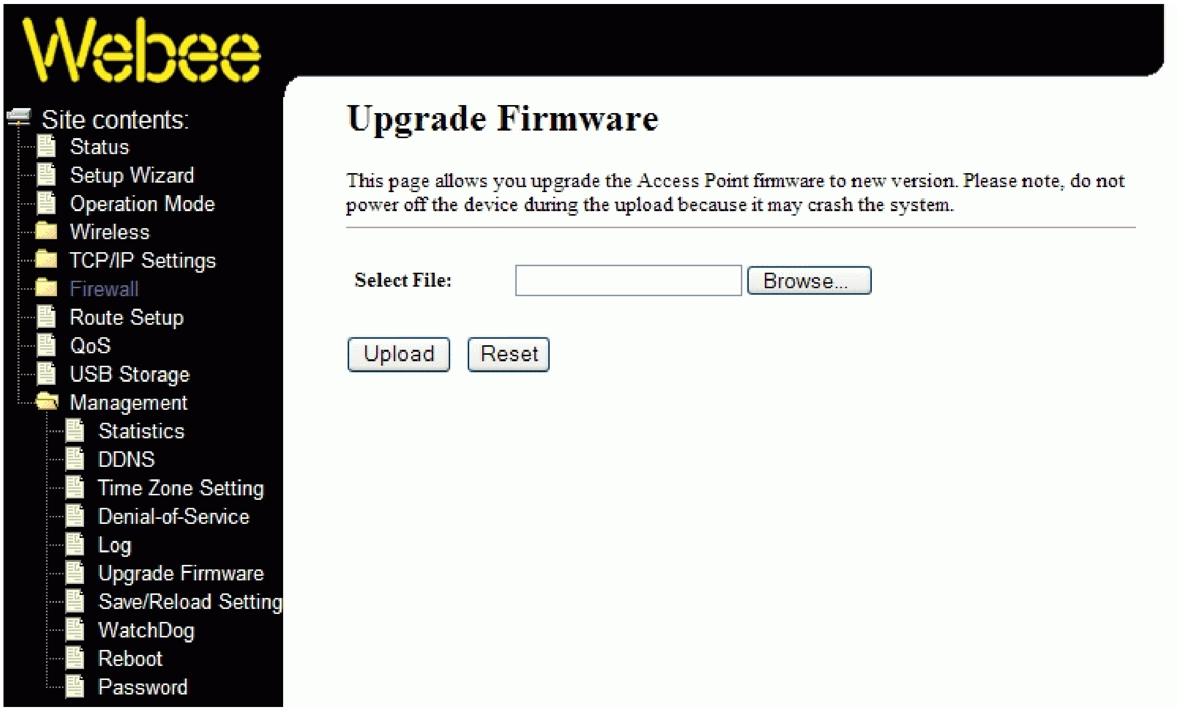
☑ system all □ wireless □ DoS □ 11s

□ Enable Remote Log Log Server IP Address:

Item	Description
Enable Log	Click the checkbox to enable log.
System all	Show all log of Webee Router
Wirelessy	Only show wireless log
DoS	Only show Denial-of-Service log
Enable Remote Log	Click the checkbox to enable remote log service.
Log Server IP Address	Input the remote log IP address
Apply Changes	Click the ***Apply Changes*** button to save above settings.
Refresh	Click the refresh the log shown on the screen.
Clear	Clear log display screen

4.3.31 Management - Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.



Upgrade Firmware

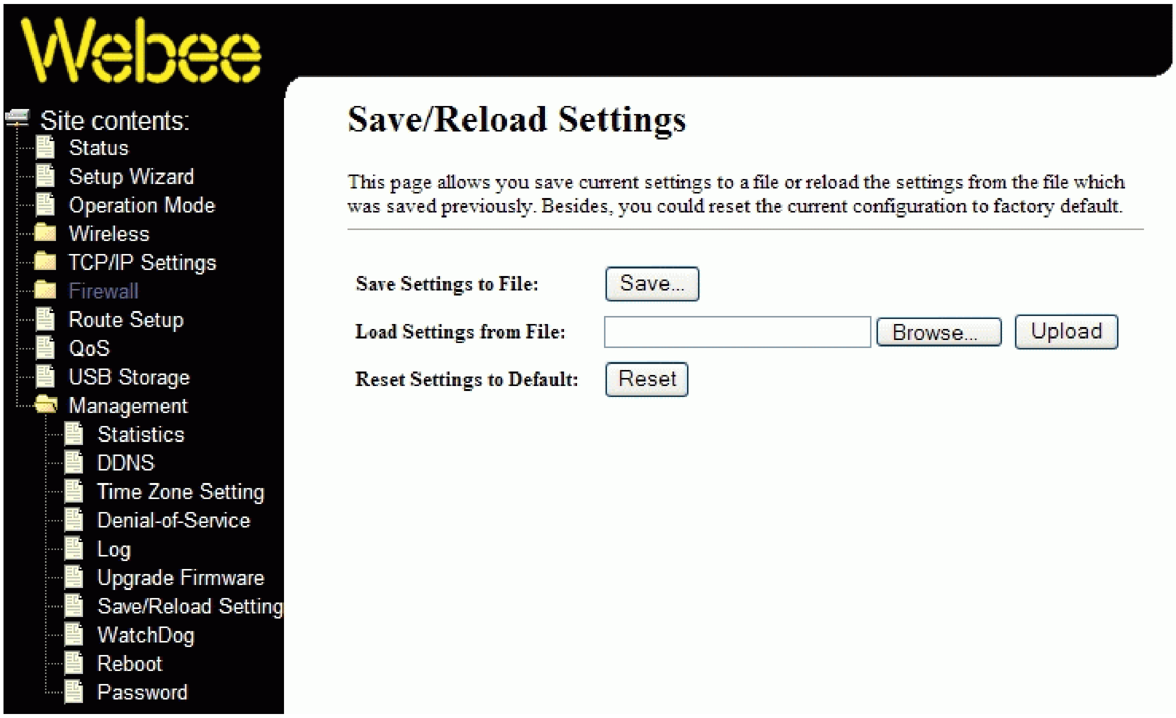
This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Select File:

Item	Description
Select File	Click the ***Browse*** button to select the new version of web firmware image file.
Upload	Click the ***Upload*** button to update the selected web firmware image to the Webee Router.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.32 Management Save/ Reload Settings

This page allows you save current settings to a file or reload the settings from the file that was saved previously. Besides, you could reset the current configuration to factory default.



Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File: Save...

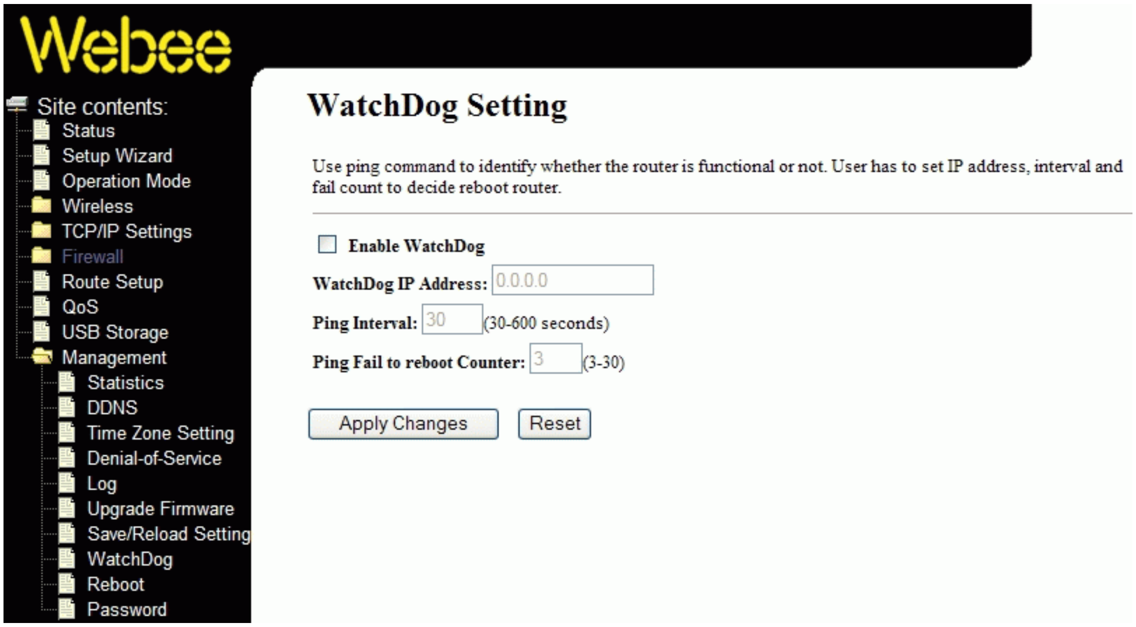
Load Settings from File: Browse... Upload

Reset Settings to Default: Reset

Item	Description
Save Settings to File	Click the ***Save*** button to download the configuration parameters to your personal computer.
Load Settings from File	Click the ***Browse*** button to select the configuration files then click the ***Upload*** button to update the selected configuration to the Webee Router.
Reset Settings to Default	Click the ***Reset*** button to reset the configuration parameter to factory defaults.

4.3.33 Management – WatchDog

Use ping command to identify whether the router is functional or not. User has to set IP address, interval and fail count to decide reboot router.



WatchDog Setting

Use ping command to identify whether the router is functional or not. User has to set IP address, interval and fail count to decide reboot router.

☐ **Enable WatchDog**

WatchDog IP Address: 0.0.0.0

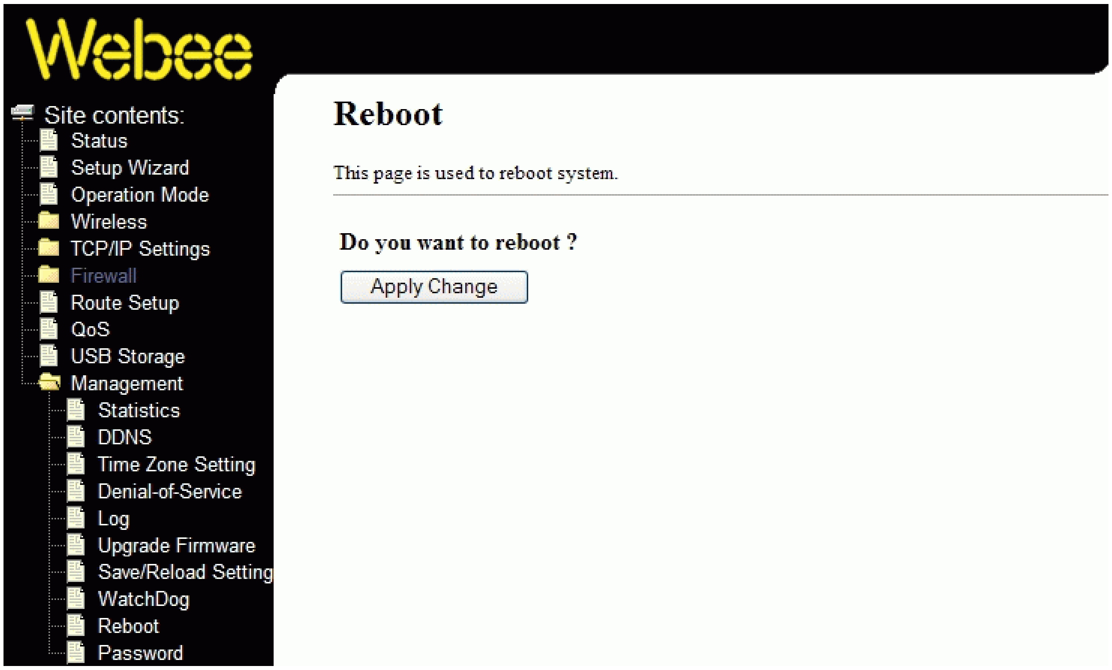
Ping Interval: 30 (30-600 seconds)

Ping Fail to reboot Counter: 3 (3-30)

Item	**Description**
Enable WatchDog	Click to Enable the WatchDog function
WatchDog IP Address	Fill in the IP address. If router don't get request form the IP address, router will restart.
Ping Interval	Set router how long to ping IP address.
Ping Fail to rebbot Counter	Set router how many times to ping IP address
Apply Changes	Click the ***Apply Changes*** button to save settings.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

4.3.34 Management – Reboot

This page is used to reboot the system.



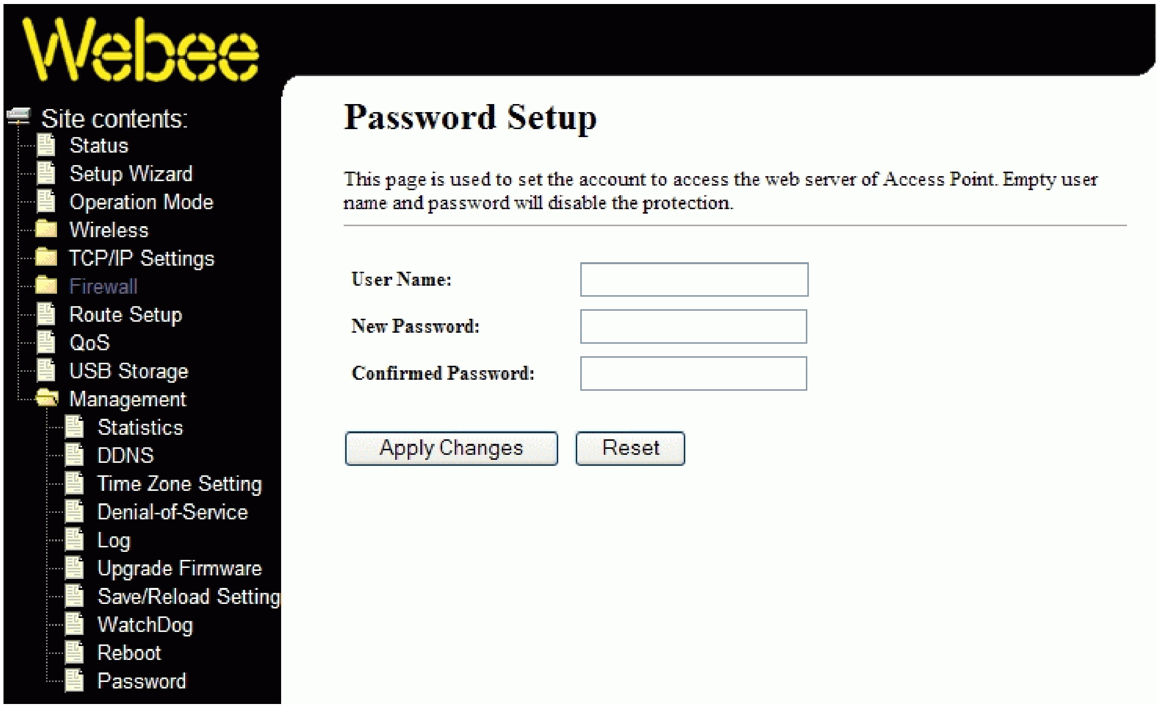
Reboot

This page is used to reboot system.

Do you want to reboot ?

4.3.35 Management - Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:	
New Password:	
Confirmed Password:	

Item	**Description**
User Name	Fill in the user name for web management login control.
New Password	Fill in the password for web management login control.
Confirmed Password	Because the password input is invisible, so please fill in the password again for confirmation purpose.
Apply Changes	Clear the ***User Name*** and ***Password*** fields to empty, means to apply no web management login control. Click the ***Apply Changes*** button to complete the new configuration setting.
Reset	Click the ***Reset*** button to abort change and recover the previous configuration setting.

5. WARRANTY AND SUPPORT

The Webee Router has a 2 year hardware warranty.

If you encounter a hardware problem during the warranty period, please contact your reseller.

For more information and support on the network services, please contact your service provider.

For more information and support on the router, you may contact the helpdesk service of the importer.

The importer will provide software updates on their web site.

Importer in Sweden
DAIMLER SWEDEN AB
www.daimler.se

Technical Support:
support@webee.se

Importer in Finland
DAIMLER FINLAND OY AB
www.daimler.fi

Technical Support:
support@daimler.fi

Tel. +358 9 5601 1234
Mon-Fri 08.30 – 16.30

Importer in Denmark
DF COM APS
www.dfcom.dk

Technical Support :
support@dfcom.dk

Importer in Estonia
DAIMLER EESTI OÜ
www.daimlereesti.ee

Technical Support:
support@daimlereesti.ee

6. FREQUENTLY ASKED QUESTIONS (FAQ)

6.1. WHAT AND HOW TO FIND MY PC'S IP AND MAC ADDRESS?

IP address is the identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 191.168.1.254 could be an IP address.

The MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

To find your PC's IP and MAC address,

- Open the Command program in the Microsoft Windows.
- Type in ***ipconfig /all*** then press the ***Enter*** button.

➢ Your PC's IP address is the one entitled IP Address and your PC's MAC address is the one entitled Physical Address.

6.2. WHAT IS WIRELESS LAN?

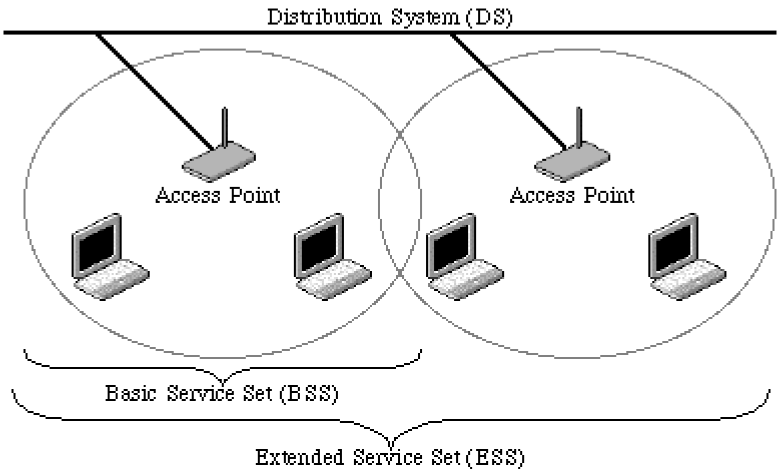
A wireless LAN (WLAN) is a network that allows access to Internet without the need for any wired connections to the user's machine.

6.3. WHAT ARE ISM BANDS?

ISM stands for Industrial, Scientific and Medical; radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 915 +/- 13 MHz, 2450 +/- 50 MHz and 5800 +/- 75 MHz.

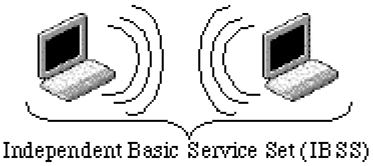
6.4. HOW DOES WIRELESS NETWORKING WORK?

The 802.11 standard define two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode.



Example 1: Wireless Infrastructure Mode

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client site).



Example 2: wireless Ad Hoc Mode

6.5. WHAT IS BSSID?

A six-byte address that distinguishes a particular a particular access point from others. Also know as just SSID. Serves as a network ID or name.

6.6. WHAT IS ESSID?

The Extended Service Set ID (ESSID) is the name of the network you want to access. It is used to identify different wireless networks.

6.7. WHAT ARE POTENTIAL FACTORS THAT MAY CAUSES INTERFERENCE?

Factors of interference:

- Obstacles: walls, ceilings, furniture… etc.
- Building Materials: metal door, aluminum studs.
- Electrical devices: microwaves, monitors and electrical motors.

Solutions to overcome the interferences:

- Minimizing the number of walls and ceilings.
- Position the WLAN antenna for best reception.
- Keep WLAN devices away from other electrical devices, eg: microwaves, monitors, electric motors, … etc.
- Add additional WLAN Access Points if necessary.

6.8. WHAT ARE THE OPEN SYSTEM AND SHARED KEY AUTHENTICATIONS?

IEEE 802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then returns a frame that indicates whether it recognizes the sending station. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

6.9. WHAT IS WEP?

An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alert frame bits to avoid disclosure to eavesdroppers.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

6.10. WHAT IS FRAGMENT THRESHOLD?

The proposed protocol uses the frame fragmentation mechanism defined in IEEE 802.11 to achieve parallel transmissions. A large data frame is fragmented into several fragments each of size equal to fragment threshold. By tuning the fragment threshold value, we can get varying fragment sizes. The determination of an efficient fragment threshold is an important issue in this scheme. If the fragment threshold is small, the overlap part of the master and parallel transmissions is large. This means the spatial reuse ratio of parallel transmissions is high. In contrast, with a large fragment threshold, the overlap is small and the spatial reuse ratio is low. However high fragment threshold leads to low fragment overhead. Hence there is a trade-off between spatial re-use and fragment overhead.

Fragment threshold is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented.

If you find that your corrupted packets or asymmetric packet reception (all send packets, for example). You may want to try lowering your fragmentation threshold. This will cause packets to be broken into smaller fragments. These small fragments, if corrupted, can be resent faster than a larger fragment. Fragmentation increases overhead, so you'll want to keep this value as close to the maximum value as possible.

6.11. WHAT IS RTS (REQUEST TO SEND) THRESHOLD?

The RTS threshold is the packet size at which packet transmission is governed by the RTS/CTS transaction. The IEEE 802.11-1997 standard allows for short packets to be transmitted without RTS/CTS transactions. Each station can have a different RTS threshold. RTS/CTS is used when the data packet size exceeds the defined RTS threshold. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

This setting is useful for networks with many clients. With many clients, and a high network load, there will be many more collisions. By lowering the RTS threshold, there may be fewer collisions, and performance should improve. Basically, with a faster RTS threshold, the system can recover from problems faster. RTS packets consume valuable bandwidth, however, so setting this value too low will limit performance.

6.12. WHAT IS BEACON INTERVAL?

In addition to data frames that carry information from higher layers, 802.11 includes management and control frames that support data transfer. The beacon frame, which is a type of management frame, provides the "heartbeat" of a wireless LAN, enabling stations to establish and maintain communications in an orderly fashion.

Beacon Interval represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).

6.13. WHAT IS PREAMBLE TYPE?

There are two preamble types defined in IEEE 802.11 specification. A long preamble basically gives the decoder more time to process the preamble. All 802.11 devices support a long preamble. The short preamble is designed to improve efficiency (for example, for VoIP systems). The difference between the two is in the Synchronization field. The long preamble is 128 bits, and the short is 56 bits.

6.14. WHAT IS SSID BROADCAST?

Broadcast of SSID is done in access points by the beacon. This announces your access point (including various bits of information about it) to the wireless world around it. By disabling that feature, the SSID configured in the client must match the SSID of the access point.

Some wireless devices don't work properly if SSID isn't broadcast (for example the D-link

DWL-120 USB 802.11b adapter). Generally if your client hardware supports operation with SSID disabled, it's not a bad idea to run that way to enhance network security. However it's no replacement for WEP, MAC filtering or other protections.

6.15. WHAT IS WI-FI PROTECTED ACCESS (WPA)?

Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer-term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the WI-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

To upgrade a WLAN network to support WPA, Access Points will require a WPA software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

6.16. WHAT IS WPA2?

It is the second generation of WPA. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

6.17. WHAT IS 802.1X AUTHENTICATION?

802.1x is a framework for authenticated MAC-level access control, defines Extensible Authentication Protocol (EAP) over LANs (WAPOL). The standard encapsulates and leverages much of EAP, which was defined for dial-up authentication with Point-to-Point Protocol in RFC 2284.

Beyond encapsulating EAP packets, the 802.1x standard also defines EAPOL messages that convey the shared key information critical for wireless security.

6.18. WHAT IS TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)?

The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

6.19. WHAT IS ADVANCED ENCRYPTION STANDARD (AES)?

Security issues are a major concern for wireless LANs, AES is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES.

6.20. WHAT IS INTER-ACCESS POINT PROTOCOL (IAPP)?

The IEEE 802.11f Inter-Access Point Protocol (IAPP) supports Access Point Vendor interoperability, enabling roaming of 802.11 Stations within IP subnet.

IAPP defines messages and data to be exchanged between Access Points and between the IAPP and high layer management entities to support roaming. The IAPP protocol uses TCP for inter-Access Point communication and UDP for RADIUS request/response exchanges. It also uses Layer 2 frames to update the forwarding tables of Layer 2 devices.

6.21. WHAT IS WIRELESS DISTRIBUTION SYSTEM (WDS)?

The Wireless Distribution System feature allows WLAN AP to talk directly to other APs via wireless channel, like the wireless bridge or repeater service.

6.22. WHAT IS UNIVERSAL PLUG AND PLAY (UPNP)?

UPnP is an open networking architecture that consists of services, devices, and control points. The ultimate goal is to allow data communication among all UPnP devices regardless of media, operating system, programming language, and wired/wireless connection.

6.23. WHAT IS MAXIMUM TRANSMISSION UNIT (MTU) SIZE?

Maximum Transmission Unit (MTU) indicates the network stack of any packet is larger than this value will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will be accepted. The actual MTU of the PPP connection will be set to the smaller one of MTU and the peer’s MRU. The default is value 1400.

6.24. WHAT IS CLONE MAC ADDRESS?

Clone MAC address is designed for your special application that request the clients to register to a server machine with one identified MAC address.
Since that all the clients will communicate outside world through the Webee Router, so have the cloned MAC address set on the Webee Router will solve the issue.

6.25. WHAT IS DDNS?

DDNS is the abbreviation of Dynamic Domain Name Server. It is designed for user own the DNS server with dynamic WAN IP address.

6.26. WHAT IS NTP CLIENT?

NTP client is designed for fetching the current timestamp from internet via Network Time protocol. User can specify time zone, NTP server IP address.

6.27.WHAT IS VPN?

VPN is the abbreviation of Virtual Private Network. It is designed for creating point-to point private link via shared or public network.

6.28. WHAT IS IPSEC?

IPSEC is the abbreviation of IP Security. It is used to transferring data securely under VPN.

6.29. WHAT IS WLAN BLOCK RELAY BETWEEN CLIENTS?

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). The access point provides a local relay function for the BSS. All stations in the BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS

6.30. WHAT IS WMM?

WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

6.31. WHAT IS WLAN ACK TIMOUT?

ACK frame has to receive ACK timeout frame. If remote does not receive in specified period, it will be retransmitted.

6.32. WHAT IS MODULATION CODING SCHEME (MCS)?

MCS is Wireless link data rate for 802.11n. The throughput/range performance of a AP will depend on its implementation of coding schemes. MCS includes variables such as the number of spatial streams, modulation, and the data rate on each stream. Radios establishing and maintaining a link must automatically negotiate the optimum MCS based on channel conditions and then continuously adjust the selection of MCS as conditions change due to interference, motion, fading, and other events.

6.33. WHAT IS FRAME AGGREGATION?

Every 802.11 packet, no matter how small, has a fixed amount of overhead associated with it. Frame Aggregation combines multiple smaller packets together to form one larger packet. The larger packet can be sent without the overhead of the individual packets. This technique helps improve the efficiency of the 802.11n radio allowing more end user data to be sent in a given time.

6.34. WHAT IS GUARD INTERVALS (GI)?

A GI is a period of time between symbol transmission that allows reflections (from multipath) from the previous data transmission to settle before transmitting a new symbol.
The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive.

7. CONFIGURATION EXAMPLES

7.1. EXAMPLE ONE – PPPOE ON THE WAN

Sales division of Company ABC likes to establish a WLAN network to support mobile communication on sales' Notebook PCs. MIS engineer collects information and plans the Webee Router implementation by the following configuration.

WAN configuration:

PPPoE

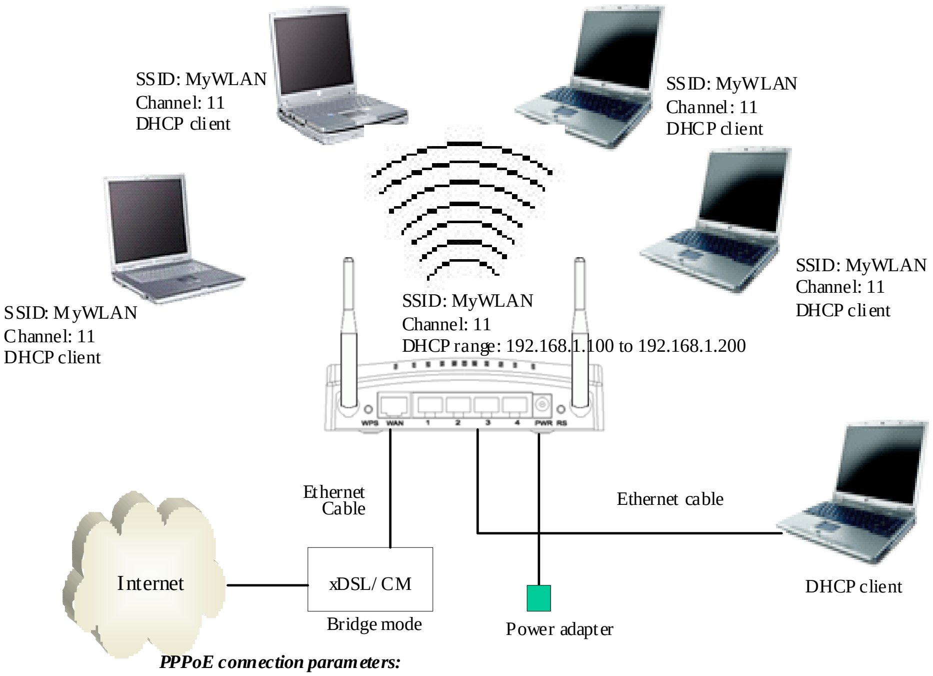
User Name	**H890123456**
Password	**PW192867543210**

LAN configuration

IP Address	**192.168.1.254**
Subnet Mask	**255.255.255.0**
Default Gateway	**0.0.0.0**
DHCP Client Range	**192.168.1.100 – 192.168.1.200**

WLAN configuration

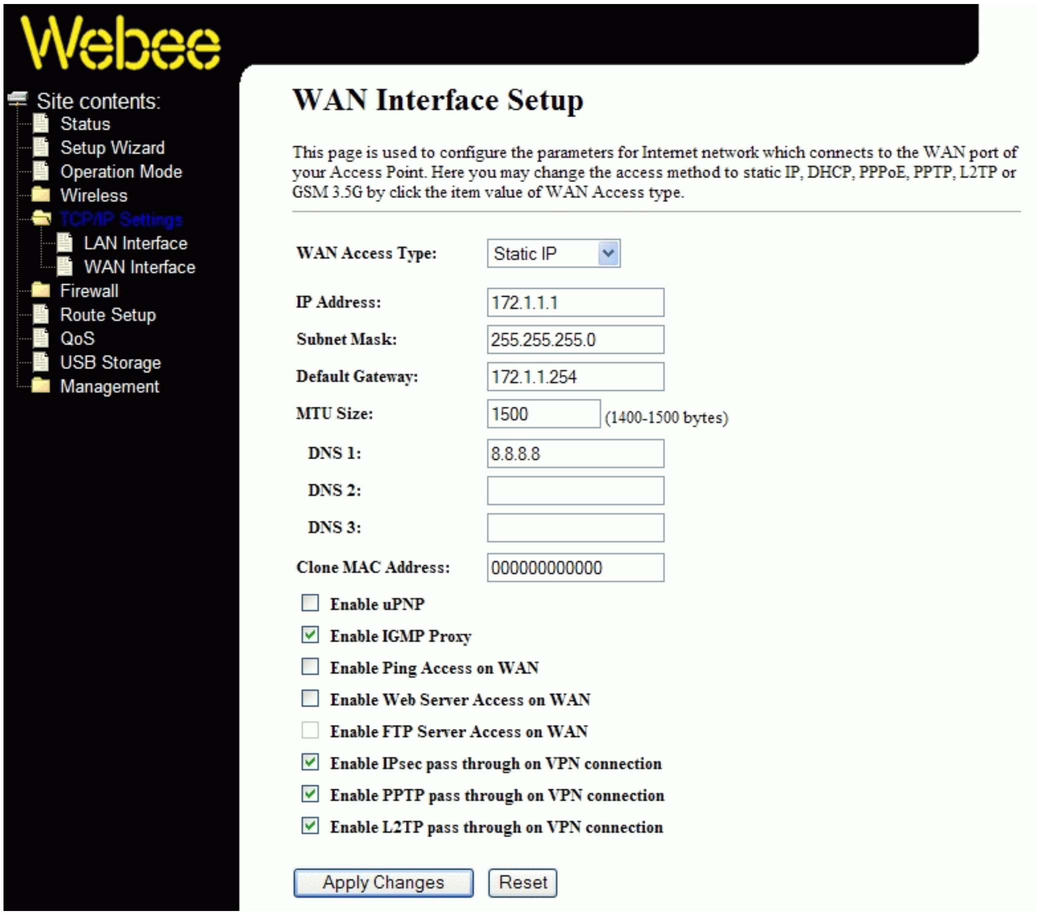
SSID	**MyWLAN**
Channel Number	**11**



PPPoE connection parameters:
User Name: H890123456
Passwrod: pw192 867543210

Configure the WAN interface:
Open WAN Interface Setup page, select PPPoE then enter the User Name "**H890123456"** and Password "**PW192867543210**", the password is encrypted to display on the screen.

Press button Apply Changes to confirm the configuration setting.



WAN Interface Setup

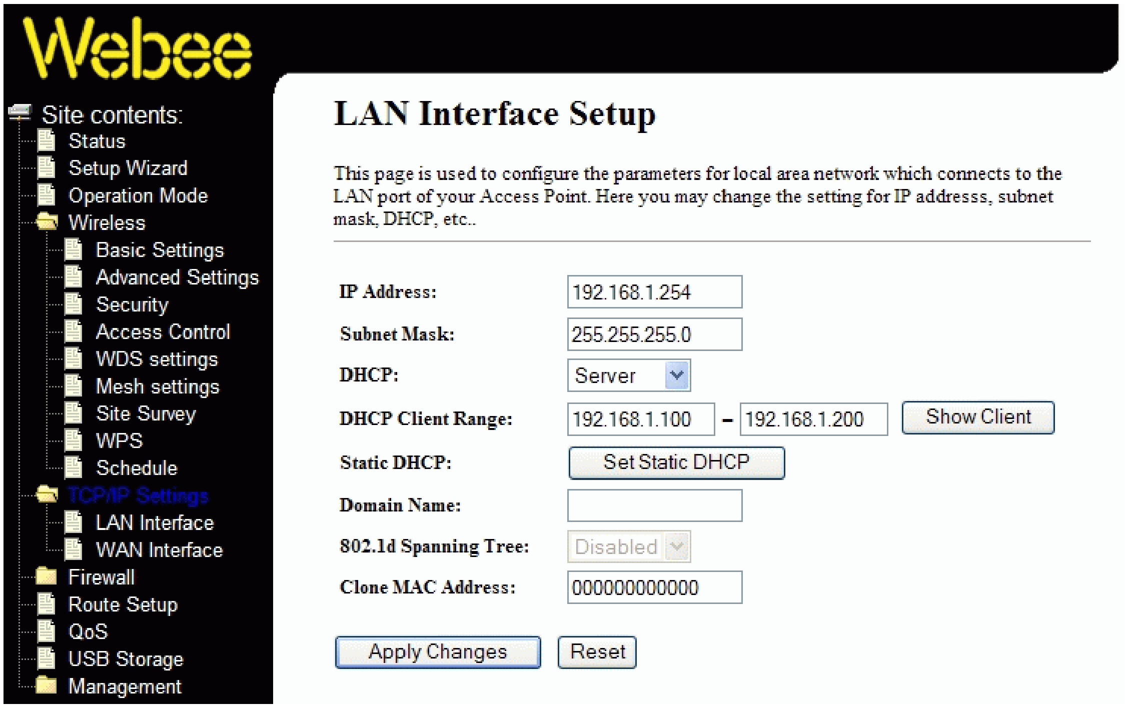
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	8.8.8.8
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

☐ Enable uPNP
☑ Enable IGMP Proxy
☐ Enable Ping Access on WAN
☐ Enable Web Server Access on WAN
☐ Enable FTP Server Access on WAN
☑ Enable IPsec pass through on VPN connection
☑ Enable PPTP pass through on VPN connection
☑ Enable L2TP pass through on VPN connection

Configure the LAN interface:
Open LAN Interface Setup page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**", Default Gateway "**0.0.0.0**", enable DHCP Server, DHCP client range "**192.168.1.100**" to "**192.168.1.200**".

Press button Apply Changes to confirm the configuration setting.



LAN Interface Setup

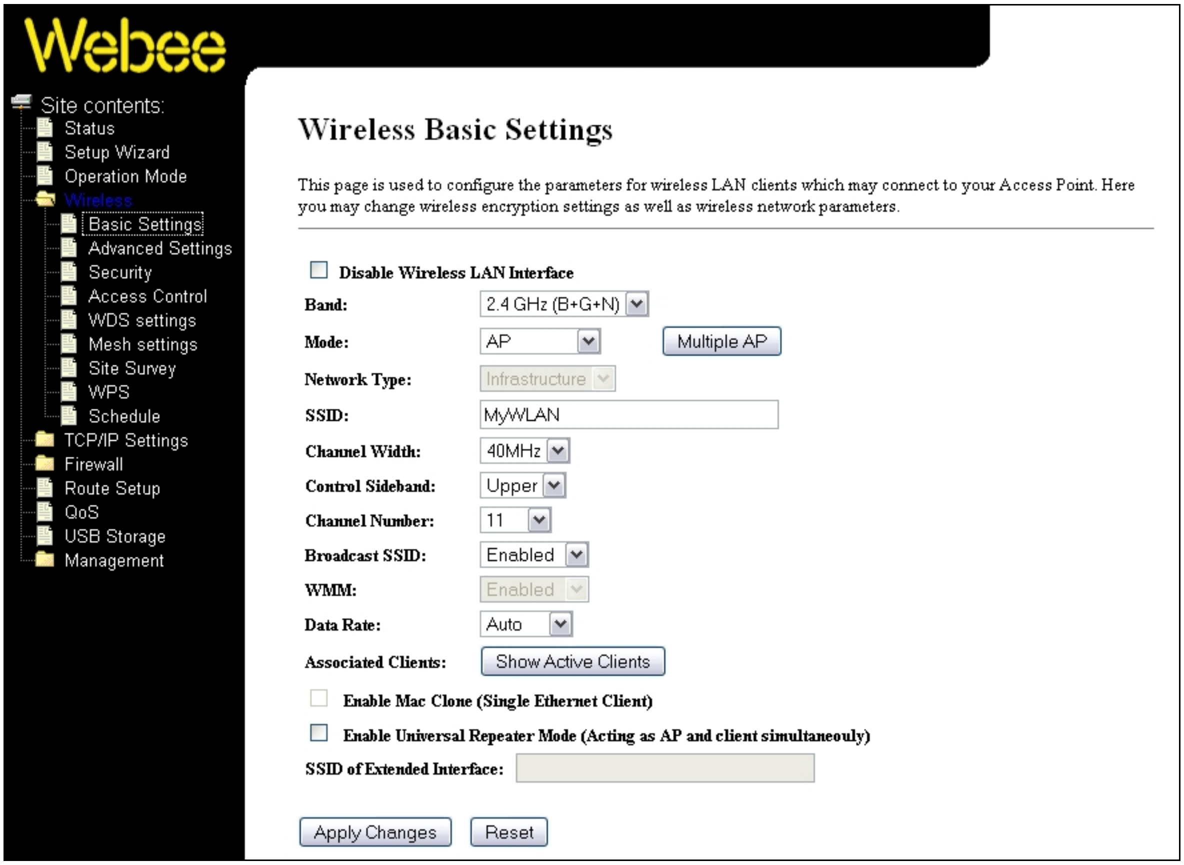
This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200 Show Client
Static DHCP:	Set Static DHCP
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Apply Changes Reset

Configure the WLAN interface:
Open WLAN Interface Setup page, enter the SSID "**MyWLAN**", Channel Number "**11**".

Press button Apply Changes to confirm the configuration setting.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	MyWLAN
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
Associated Clients:	Show Active Clients

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

7.2. EXAMPLE TWO – FIXED IP ON THE WAN

Company ABC likes to establish a WLAN network to support mobile communication on all employees’ Notebook PCs. MIS engineer collects information and plans the Webee Router implementation by the following configuration.

WAN configuration:

Fixed IP

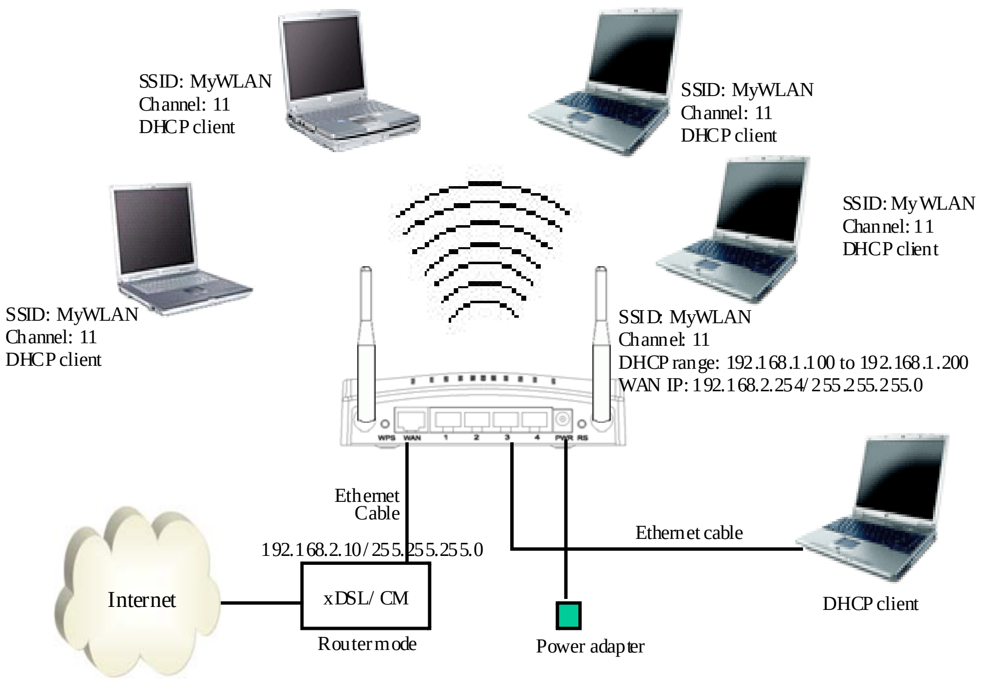
IP Address	**192.168.2.254**
Subnet Mask	**255.255.255.0**
Default Gateway	**192.168.2.10**
DNS Address	**168.95.1.1**

LAN configuration

IP Address	**192.168.1.254**
Subnet Mask	**255.255.255.0**
Default Gateway	**192.168.2.254**
DHCP Client Range	**192.168.1.100 – 192.168.1.200**

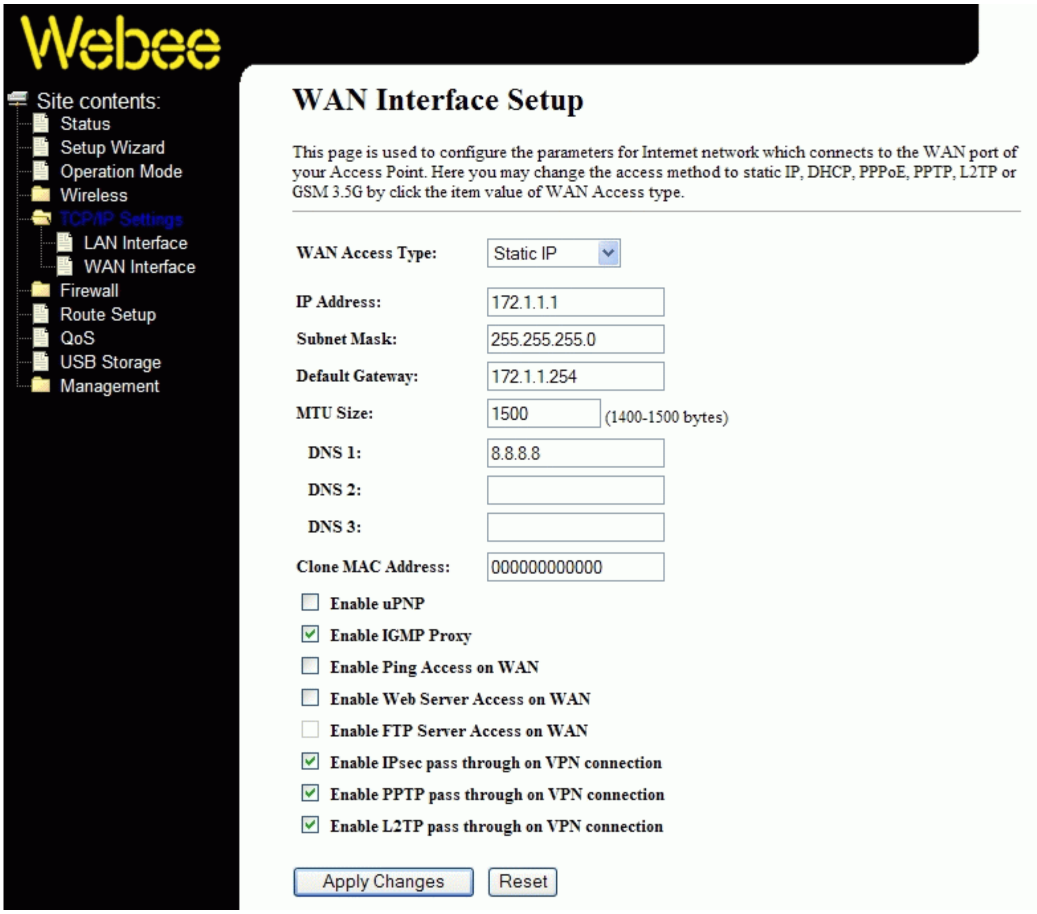
WLAN configuration

SSID	**MyWLAN**
Channel Number	**11**



Configure the WAN interface:
Open WAN Interface Setup page, select Fixed IP then enter IP Address "**192.168.2.254",** subnet mask "**255.255.255.0**", Default gateway "**192.168.2.10**".

Press button Apply Changes to confirm the configuration the setting.



WAN Interface Setup

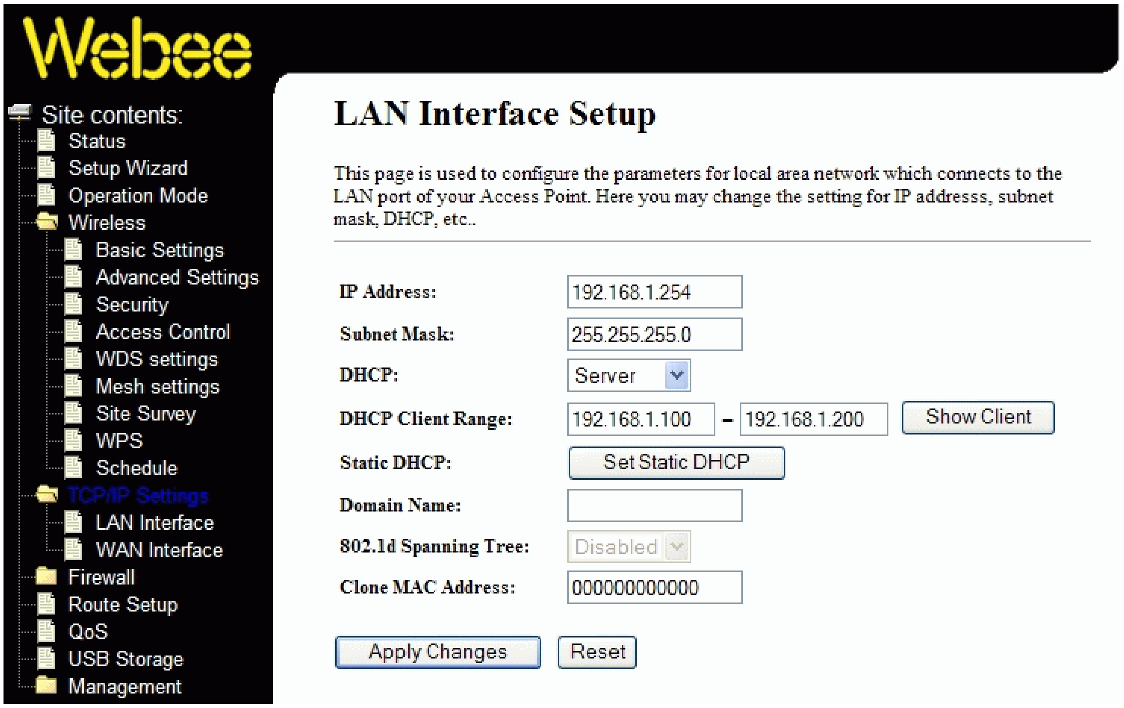
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP, L2TP or GSM 3.5G by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	8.8.8.8
DNS 2:	
DNS 3:	
Clone MAC Address:	000000000000

□ **Enable uPNP**
☑ **Enable IGMP Proxy**
□ **Enable Ping Access on WAN**
□ **Enable Web Server Access on WAN**
□ **Enable FTP Server Access on WAN**
☑ **Enable IPsec pass through on VPN connection**
☑ **Enable PPTP pass through on VPN connection**
☑ **Enable L2TP pass through on VPN connection**

Configure the LAN interface:
Open LAN Interface Setup page, enter the IP Address "**192.168.1.254**", Subnet Mask "**255.255.255.0**", enable DHCP Server, DHCP client range "**192.168.1.100**" to "**192.168.1.200**".

Press button Apply Changes to confirm the configuration setting.



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0
DHCP:	Server
DHCP Client Range:	192.168.1.100 – 192.168.1.200
Static DHCP:	
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Configure the WLAN interface:
Open WLAN Interface Setup page, enter the SSID “**MyWLAN**”, Channel Number **“11”.**

Press button Apply Changes to confirm the configuration setting.

DECLARATION OF CONFORMITY

We confirm that the product fulfills the requirements of the R&TTE Directive (1999/5/EC)

Type: Webee Wireless N Router

The product is marked with the CE marking, Notified Body number and equipment class identifier according to the Directive 1999/5/EC.

The construction of the appliance is in accordance with the following harmonized standards:

EN 300 328 V1.7.1
EN 301 489-1 V1.7.1, EN 301 489-17 V1.3.2
EN 301 489-17 V1.3.2
EN 60950-1: 2006
MPE calculation

The following importer is responsible for this declaration:

Daimler Finland Oy Ab

Kutomotie 18 B
FI-00380 Helsinki Finland

Helsinki 1.6.2010